ProCurve
Networking by HP

Users' Guide

ProCurve Network Access Controller 800

www.procurve.com

hp invent

ProCurve
Network Access Controller 800

Release 1.0

Users Guide

© Copyright 2007 Hewlett-Packard Development Company, L.P. All Rights Reserved.

This document contains information which is protected by copyright. Reproduction, adaptation, or translation without prior permission is prohibited, except as allowed under the copyright laws.

Publication Number

5991-8571
August 2007

(rev-h)

Trademark Credits

Microsoft, Windows, Windows 95, and Microsoft Windows NT are registered trademarks of Microsoft Corporation. Internet Explorer is a trademark of Microsoft Corporation. Ethernet is a registered trademark of Xerox Corporation. Netscape is a registered trademark of Netscape Corporation.

Disclaimer

The information contained in this document is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California 95747-5551
http://www.hp.com/go/hpprocurve

Contents

1 Introduction

What you Need to get Started 1-2
NAC 800 Home Window 1-4
System Monitor 1-6
Overview 1-8
The NAC 800 Process 1-10
About NAC 800 1-10
NAC Policy Definition 1-10
Endpoint Testing 1-11
Compliance Enforcement 1-12
Automated and Manual Repair 1-12
Targeted Reporting 1-12
Technical Support 1-13
Additional Documentation 1-14
Upgrading 1-15
Conventions Used in This Document 1-16
Navigation Paragraph 1-16
Tip Paragraph 1-16
Note Paragraph 1-16
Caution Paragraph 1-16
Warning Paragraph 1-17
Bold Font 1-17
Task Paragraph 1-17
Italic Text 1-17
Courier Font 1-18
Angled Brackets 1-18
Square Brackets 1-18
Terms 1-19
Copying Files 1-20
SCP 1-20
PSCP 1-20

2 Clusters and Servers

Overview 2-2
Installation Examples 2-3

Single-server Installation 2-3
Multiple-server Installations 2-3

3 System Configuration

Introduction 3-4
Enforcement Clusters and Servers 3-6
Enforcement Clusters 3-7
Adding an Enforcement Cluster 3-7
Editing Enforcement Clusters 3-9
Viewing Enforcement Cluster Status 3-10
Deleting Enforcement Clusters 3-11
Enforcement Servers 3-13
Adding an Enforcement Server 3-13
Cluster and Server Icons 3-15
Editing Enforcement Servers 3-15
Changing the Enforcement Server Network Settings 3-17
Changing the Enforcement Server Date and Time 3-17
Modifying the ES root Account Password 3-18
Viewing Enforcement Server Status 3-18
Deleting Enforcement Servers 3-20
Enforcement Server Recovery 3-20
Management Server 3-21
Viewing Network Settings 3-21
Modifying Management Server Network Settings 3-23
Selecting a Proxy Server 3-23
Setting the Date and Time 3-24
Automatically Setting the Time 3-25
Manually Setting the Time 3-25
Selecting the Time Zone 3-26
Changing MS SNMP Settings 3-26
Modifying the MS root Account Password 3-26
Checking for NAC 800 Upgrades 3-27
Changing the NAC 800 Console Timeout 3-27
User Accounts 3-29
Adding a User Account 3-29
Searching for a User Account 3-32
Sorting the User Account Area 3-33
Copying a User Account 3-33
Editing a User Account 3-34
Deleting a User Account 3-35

User Roles 3-37
Adding a User Role 3-37
Editing User Roles 3-40
Deleting User Roles 3-41
Sorting the User Roles Area 3-42
License 3-43
Updating Your License 3-43
Test Updates 3-45
Manually Checking for Test Updates 3-45
Selecting Test Update Times 3-46
Viewing Test Update Logs 3-47
Quarantining 3-49
Selecting the Quarantine Method 3-49
Entering Basic 802.1X Settings 3-51
Selecting the RADIUS Authentication method 3-51
Configuring Windows Domain Settings 3-52
Configuring OpenLDAP Settings 3-54
Configuring Novell eDirectory Settings 3-57
Adding 802.1X Devices 3-60
Testing the Connection to a Device 3-61
Cisco IOS 3-62
Cisco CatOS 3-63
Enterasys 3-65
Extreme ExtremeWare 3-67
Extreme XOS 3-69
Foundry 3-71
HP ProCurve Switch 3-73
HP ProCurve WESM 3-76
HP ProCurve 420 AP or HP ProCurve 530 AP 3-79
Nortel 3-81
Other 3-83
Setting DHCP Enforcement 3-85
Adding a DHCP Quarantine Area 3-87
Sorting the DHCP Quarantine Area 3-89
Editing a DHCP Quarantine Area 3-89
Deleting a DHCP Quarantine Area 3-90
Maintenance 3-91
Initiating a New Backup 3-91
Restoring From a Backup 3-93
Downloading Support Packages 3-94

Cluster Setting Defaults 3-95
Testing Methods 3-95
Selecting Test Methods 3-95
Ordering Test Methods 3-96
Recommended Test Methods 3-97
Selecting End-user Options 3-98
Accessible Services 3-98
Exceptions 3-100
Always Granting Access to Endpoints and Domains 3-101
Always Quarantine Endpoints and Domains 3-102
Notifications 3-102
Enabling Notifications 3-102
End-user Screens 3-104
Specifying an End-user Screen Logo 3-104
Specifying the End-user Screen Text 3-105
Specifying the End-user Test Failed Pop-up Window 3-106
Agentless Credentials 3-107
Adding Windows Credentials 3-107
Testing Windows Credentials 3-109
Editing Windows Credentials 3-109
Deleting Windows Credentials 3-110
Sorting the Windows Credentials Area 3-110
Logging 3-111
Setting ES Logging Levels 3-111
Setting 802.1X Devices Logging Levels 3-112
Setting IDM Logging Levels 3-112
Advanced Settings 3-114
Setting the Agent Read Timeout 3-114
Setting the RPC Connection Timeout 3-114
Setting the RPC Command Timeout 3-115

4 Endpoint Activity

Overview 4-2
Filtering the Endpoint Activity Window 4-4
Filtering by Access Control or Test Status 4-4
Filtering by Time 4-5
Limiting Number of Endpoints Displayed 4-6
Searching 4-7
Access Control States 4-9
Test Status States 4-10
Viewing Endpoint Access Status 4-14

Selecting Endpoints to Act on 4-15
Acting on Selected Endpoints 4-16
Manually Retest an Endpoint 4-16
Immediately Grant Access to an Endpoint 4-16
Immediately Quarantine an Endpoint 4-17
Clearing Temporary Endpoint States 4-17
Viewing Endpoint Information 4-18

5 End-user Access

Overview 5-2
Endpoints Supported 5-3
Browser Version 5-4
Browser Settings 5-5
Agentless Settings 5-6
Ports Used for Testing 5-8
Firewall Settings 5-9
Managed Endpoints 5-9
Unmanaged Endpoints 5-9
Allowing the Windows RPC Service Through the Firewall 5-9
Allowing NAC 800 through the OS X Firewall 5-12
End-user Access Windows 5-15
Opening Window 5-16
Windows NAC Agent Test Windows 5-17
Automatically Installing the Windows Agent 5-17
Removing the Agent 5-20
Manually Installing the Windows Agent 5-20
How to View the Windows Agent Version Installed 5-21
Mac OS Agent Test Windows 5-22
Installing the MAC OS Agent 5-22
Verifying the Mac OS Agent 5-25
Removing the Mac OS Agent 5-29
ActiveX Test Windows 5-30
Agentless Test Windows 5-30
Testing Window 5-33
Test Successful Window 5-34
Temporary Quarantine Window 5-35
Testing Cancelled Window 5-36
Testing Failed Window 5-37
Setting the Temporary Access Period 5-38
Error Windows 5-38

Customizing Error Messages 5-40

6 NAC Policies

Overview 6-2
Standard NAC Policies 6-4
NAC Policy Group Tasks 6-5
Add a NAC Policy Group 6-5
Editing a NAC Policy Group 6-5
Deleting a NAC Policy Group 6-6
NAC Policy Tasks 6-7
Enabling or Disabling an NAC Policy 6-7
Selecting the Default NAC Policy 6-7
Creating a New NAC Policy 6-7
Editing a NAC Policy 6-12
Copying a NAC Policy 6-12
Deleting a NAC Policy 6-13
Moving a NAC Policy Between NAC Policy Groups 6-13
Assigning Endpoints and Domains to a Policy 6-13
NAC Policy Hierarchy 6-14
Setting Retest Time 6-14
Setting Connection Time 6-14
Defining Non-supported OS Access Settings 6-15
Setting Test Properties 6-15
Selecting Action Taken 6-15
About NAC 800 Tests 6-17
Viewing Information About Tests 6-17
Selecting Test Properties 6-17
Entering Software Required/Not Allowed 6-17
Entering Service Names Required/Not Allowed 6-18
Entering the Browser Version Number 6-19
Test Icons 6-19

7 Quarantined Networks

Endpoint Quarantine Precedence 7-2
Using Ports in Accessible Services and Endpoints 7-4
Determining Accessible Services Example 7-6
Always Granting Access to an Endpoint 7-13
Always Quarantining an Endpoint 7-15
New Users 7-16
Shared Resources 7-17

Untestable Endpoints and DHCP Mode 7-18

8 High Availability and Load Balancing

High Availability 8-2
Load Balancing 8-6

9 Inline Quarantine Method

Inline 9-2

10 DHCP Quarantine Method

Overview 10-2
Configuring NAC 800 for DHCP 10-4
Setting Up a Quarantine Area 10-4
Router Configuration 10-4
Configuring the Router ACLs 10-5
Configuring Windows Update Service for XP SP2 10-5

11 802.1X Quarantine Method

About 802.1X 11-2
NAC 800 and 802.1X 11-4
Setting Up the 802.1X Components 11-7
Setting up the RADIUS Server 11-7
Using the NAC 800 IAS Plug-in to the Microsoft IAS RADIUS Server . 11-7
Configuring the Microsoft IAS RADIUS server 11-10
Proxying RADIUS Requests to an Existing RADIUS Server Using the Built-in NAC 800 RADIUS Server 11-37
Using the Built-in NAC 800 RADIUS Server for Authentication . . 11-40
Configuring Non-HP Switches 11-40
Enabling NAC 800 for 802.1X 11-43
NAC 800 Console Configuration 11-43
Setting Up the Supplicant 11-44

Setting Up the Authenticator 11-47
Cisco® 2950 IOS 11-47
Cisco® 4006 CatOS 11-48
Enterasys® Matrix 1H582-25 11-49
Extreme® Summit 48si 11-49
ExtremeWare 11-50
ExtremeXOS 11-50
Foundry® FastIron® Edge 2402 11-51
HP ProCurve® 420AP 11-51
HP ProCurve® 530AP 11-52
HP ProCurve® 3400/3500/5400 11-53
Nortel® 5510 11-54

12 Reports

Report Types 12-2
Generating Reports 12-4
Viewing Report Details 12-6
Printing Reports 12-7
Saving Reports to a File 12-8
Converting an HTML Report to a Word Document 12-9

13 System Administration

Launching NAC 800 13-3
Launching and Logging into NAC 800 13-3
Logging out of NAC 800 13-3
Important Browser Settings 13-3
Downloading New Tests 13-4
System Settings 13-5
Matching Windows Domain Policies to NAC Policies 13-5
Setting the Access Mode 13-5
Naming your Enforcement Cluster 13-6
Changing the MS Host Name 13-6
Changing the ES Host Name 13-6
Resetting your System 13-6
Changing Properties 13-7
Specifying an Email Server for Sending Notifications 13-8
Windows 2003 Server Settings 13-8
Entering Networks Using CIDR Format 13-9
Database 13-10
Creating a Backup File 13-10

Restoring from Backup 13-10
Restoring the Original Database 13-11
Generating a Support Package 13-11
Supported VPNs 13-12
Adding Custom Tests 13-13
Introduction 13-13
References 13-13
Changing the Error Messages in a Test Script 13-13
Creating a Custom Test Class Script from Scratch 13-18
BasicTests API 13-28
End-user Access Windows 13-33
How NAC 800 Handles Static IP Addresses 13-34
Managing Passwords 13-35
Resetting the NAC 800 Server Password 13-36
Serial Console 13-36
Reset Appliance Mode 13-37
Resetting the NAC 800 Database Password 13-37
Changing the NAC 800 Administrator Password 13-37
Working with Ranges 13-39
Creating and Replacing SSL Certificates 13-41
Creating a New Self-signed Certificate 13-42
Using an SSL Certificate from a known Certificate Authority (CA) . . . 13-43
Moving an ES from One MS to Another 13-45
Recovering Quickly from a Network Failure 13-46

A Tests Help

Overview A-3
Browser Security Policy – Windows A-4
Browser Version A-5
Description A-5
Test Properties A-5
How Does this Affect Me? A-6
What Do I Need to Do? A-6
Internet Explorer (IE) Internet Security Zone A-6
Description A-6
Test Properties A-6
How Does this Affect Me? A-7
What Do I Need to Do? A-7

Internet Explorer (IE) Local Intranet Security Zone A-7
Description A-7
Test Properties A-7
How Does this Affect me? A-8
What Do I Need to Do? A-8
Internet Explorer (IE) Restricted Site Security Zone A-8
Description A-8
Test Properties A-8
How Does this Affect Me? A-9
What Do I Need to Do? A-9
Internet Explorer (IE) Trusted Sites Security Zone A-10
Description A-10
Test properties A-10
Operating System – Windows A-11
IIS Hotfixes A-11
Description A-11
Test Properties A-11
How Does this Affect Me? A-11
What Do I Need to Do? A-11
Internet Explorer Hotfixes A-11
Description A-11
Test Properties A-12
How Does this Affect Me? A-12
What Do I Need to Do? A-12
MVM Hotfixes A-12
Description A-12
Test Properties A-12
How Does this Affect Me? A-12
What Do I Need to Do? A-12
Service Packs A-13
Description A-13
Test Properties A-13
How Does this Affect Me? A-13
What Do I Need to Do? A-13
Windows 2000 Hotfixes A-13
Description A-13
Test Properties A-13
How Does this Affect Me? A-13
What Do I Need to Do? A-14

Windows Media Player Hotfixes A-14
Description A-14
Test Properties A-14
How Does this Affect Me? A-14
What Do I Need to Do? A-14
Windows Server 2003 SP1 Hotfixes A-14
Description A-14
Test Properties A-14
How Does this Affect Me? A-15
What Do I Need to Do? A-15
Windows Server 2003 SP2 Hotfixes A-15
Description A-15
Test Properties A-15
How Does this Affect Me? A-15
What Do I Need to Do? A-15
Windows Server 2003 Hotfixes A-15
Description A-15
Test Properties A-16
How Does this Affect Me? A-16
What Do I Need to Do? A-16
Windows XP SP2 Hotfixes A-16
Description A-16
Test Properties A-16
How Does this Affect Me? A-16
What Do I Need to Do? A-16
Windows XP Hotfixes A-17
Description A-17
Test Properties A-17
How Does this Affect Me? A-17
What Do I Need to Do? A-17
Windows Automatic Updates A-17
Description A-17
Test Properties A-17
How Does this Affect Me? A-18
What Do I Need to Do? A-18
Security Settings – OS X A-19
Mac AirPort Preference A-19
Description A-19
Test Properties A-19
How Does this Affect Me? A-19
What Do I Need to Do? A-19

Mac AirPort User Prompt A-19
Description A-19
Test Properties A-19
How Does this Affect Me? A-19
What Do I Need to Do? A-20
Mac AirPort WEP Enabled A-20
Description A-20
Test Properties A-20
How Does this Affect Me? A-20
What Do I Need to Do? A-20
Mac Bluetooth A-20
Description A-20
Test Properties A-20
How Does this Affect Me? A-21
What Do I Need to Do? A-21
Mac Firewall A-21
Description A-21
Test Properties A-21
How Does this Affect Me? A-21
What Do I Need to Do? A-21
Mac Internet Sharing A-22
Description A-22
Test Properties A-22
How Does this Affect Me? A-22
What Do I Need to Do? A-22
Mac Services A-22
Description A-22
Test Properties A-22
How Does this Affect Me? A-22
What Do I Need to Do? A-23
Security Settings – Windows A-24
Allowed Networks A-24
Description A-24
Test Properties A-24
How Does this Affect Me? A-24
What Do I Need to Do? A-24
MS Excel Macros A-24
Description A-24
Test Properties A-24
How Does this Affect Me? A-25
What Do I Need to Do? A-25

MS Outlook Macros A-25
Description A-25
Test Properties A-25
How Does this Affect Me? A-26
What Do I Need to Do? A-26
MS Word Macros A-26
Description A-26
Test Properties A-26
How Does this Affect Me? A-27
What Do I Need to Do? A-27
Services Not Allowed A-27
Description A-27
Test Properties A-27
How Does this Affect Me? A-27
What do I need to do? A-28
Services Required A-28
Description A-28
Test Properties A-28
How Does this Affect Me? A-29
What Do I Need to Do? A-29
Windows Bridge Network Connection A-29
Description A-29
Test Properties A-30
How Does this Affect Me? A-30
What Do I Need to Do? A-30
Windows Security Policy A-30
Description A-30
Test Properties A-30
How Does this Affect Me? A-31
What Do I Need to Do? A-31
Windows Startup Registry Entries Allowed A-32
Description A-32
Test Properties A-32
How Does this Affect Me? A-32
What Do I Need to Do? A-33
Software – Windows A-34
Anti-spyware A-34
Description A-34
Test Properties A-34
How Does this Affect Me? A-34
What Do I Need to Do? A-34

Anti-virus A-35
Description A-35
Test Properties A-35
How Does this Affect Me? A-35
What Do I Need to Do? A-35
High-risk Software A-36
Description A-36
Test Properties A-36
How Does this Affect Me? A-36
What Do I Need to Do? A-36
MS Office Version Check A-36
Description A-36
Test Properties A-36
How Does this Affect Me? A-36
What Do I Need to Do? A-36
P2P A-37
Description A-37
Test Properties A-37
How Does this Affect Me? A-37
What Do I Need to Do? A-37
Personal Firewalls A-37
Description A-37
Test Properties A-37
How Does this Affect Me? A-38
What Do I Need to Do? A-38
Software Not Allowed A-38
Description: A-38
How Does this Affect Me? A-38
What Do I Need to Do? A-39
Software Required A-39
Description A-39
Test Properties A-39
How Does this Affect Me? A-39
What Do I Need to Do? A-39
Worms, Viruses, and Trojans A-39
Description: A-39
Test Properties A-40
How Does this Affect Me? A-40
What Do I Need to Do? A-40

B Important Browser Settings

Pop-up Windows B-2
Active Content B-3

Minimum Font Size B-5
Page Caching B-6
Temporary Files B-7

C Installation and Configuration Check List

Minimum System Requirements C-2
IP Addresses, Hostname, Logins, and Passwords C-3
Single-server Installation C-3
Multiple-server Installations C-3
Management Server C-3
Enforcement Server 1 . . . . . C-4
Enforcement Server 2 . . . . . C-5
Enforcement Server 3 . . . . . C-5
Proxy Server C-6
Agentless Credentials C-7
Quarantine C-8
802.1X C-8
802.1X Devices C-9
DHCP C-10
Accessible services C-10
Notifications C-12
Test Exemptions C-13

D Glossary

Index

(This page intentionally left blank.)

1

Introduction

Chapter Contents

What you Need to get Started 1-2
NAC 800 Home Window 1-4
System Monitor 1-6
Overview 1-8
- The NAC 800 Process 1-10
- About NAC 800 1-10

Technical Support 1-13
Additional Documentation 1-14
Upgrading 1-15
Conventions Used in This Document 1-16
- Navigation Paragraph 1-16
- Tip Paragraph 1-16
- Note Paragraph 1-16
- Caution Paragraph 1-16
- Warning Paragraph 1-17
- Bold Font 1-17
- Task Paragraph 1-17
- Italic Text 1-17
- Courier Font 1-18
- Angled Brackets 1-18
- Square Brackets 1-18
- Terms 1-19

Copying Files 1-20
- SCP 1-20
- PSCP 1-20

What you Need to get Started

The following hardware and software is required to operate NAC 800:

- One or more ProCurve NAC 800 appliances
- Configuration information – See "Installation and Configuration Check List" on page C-1
- An Internet connection or a web proxy server that allows outbound HTTPS communications from the MS
- Workstation – A workstation running one of the following browsers with 128-bit encryption:
  - Windows –
    Mozilla version 1.7
    Mozilla Firefox version 1.5 or later
    Internet Explorer 6.0
  - Linux –
    Mozilla version 1.7
    Mozilla Firefox version 1.5 or later
- A ProCurve NAC Implementation Start-up Service, from an authorized ProCurve partner or ProCurve.
- A ProCurve NAC Endpoint Integrity Agent License

ProCurve NAC 800 is delivered as a hardware appliance that you install in your network. After NAC 800 is installed in your network, you configure it using a workstation with browser software installed.

The browser software must be configured as described in "Important Browser Settings" on page B-1.

The following documents provide information on installation and configuration, and are available at www.procurve.com/nactools:

1. *ProCurve Network Access Controller 800 Hardware Installation Guide* – Refer to this document first to see how to prepare for and perform the physical installation of the appliance and how to establish initial management access. This document contains appliance specifications, safety information, and appliance certifications.
2. *ProCurve Network Access Controller 800 Configuration Guide* – Refer to this document second, to understand the product's features, capabilities, and use. This document explains how to configure the appliance based on the usage model you choose to deploy in your network.

3. *ProCurve Network Access Controller 800Users' Guide* – Refer to this document last for information on configuring, monitoring activities, creating NAC policies, and running reports.

NAC 800 Home Window

The NAC 800 **Home** window (figure 1-1) is a centralized management console that allows you to quickly assess the status of your network. The following list and figure describe and show the key features:

1. Important status announcements – If there is anything that needs your immediate attention, a status announcement is displayed at the top of the window. Click **clear** to remove the announcement.
2. Username's account – Click this icon to open the user account editing window. See "User Accounts" on page 3-29 for details on creating and editing user accounts. You must have administrator privileges to create user accounts; however, any user can edit their own account.
3. Top 5 failed tests area – The **Top 5 failed tests** area indicates the tests that fail the most. Click on an endpoint number or the **Test results report** option to view details.
4. Window actions – Use these links to refresh the window, log out of the console, and access online help.
5. Navigation pane – The menu items shown in this pane vary depending on your permission level. See "User Roles" on page 3-37 for more information on permissions. You must have administrator privileges to create and edit user roles. Once you select a menu item from the navigation pane, use the bread crumbs at the top of the windows to navigate throughout the console (see figure 1-2. System Monitor Window on page 1-7).
6. Endpoint test status area – The **Endpoint tests** area displays the total number of endpoints that NAC 800 has attempted to test, and what the test status is for each endpoint. Click the number of endpoints to view details.
7. Access control status area – The **Access control** area displays the total number of endpoints that have attempted to connect to your network, and what the access state is as a percentage and as a number. Click on the number of endpoints to view details.
8. Enforcement server status area – The **Enforcement server status** area provides status on your Enforcement servers. Click the **System monitor** option to view details.

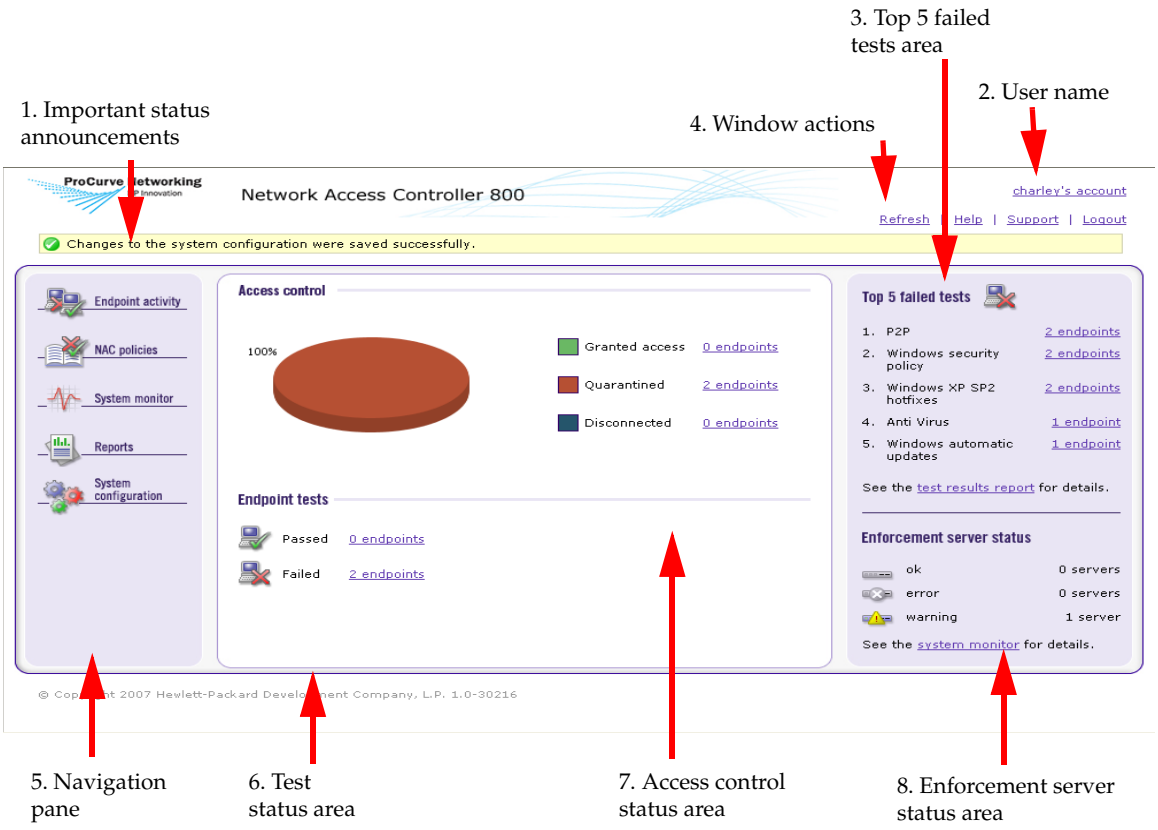


Figure 1-1. NAC 800 Home Window

System Monitor

The System monitor window provides the following information:

- Enforcement cluster name – The Enforcement clusters are listed by name in the order they were created. Click on a cluster name to view cluster details. You must have cluster-editing permissions to view and edit cluster details.
- Server name by cluster – The servers for each cluster are listed by name in the order they were created. Click on a server name to view server details. You must have cluster-editing permissions to view and edit server details.
- Cluster access mode – The cluster access mode is either **normal**, **allow all**, or **quarantine all**. See "Enforcement Clusters and Servers" on page 3-6 for instructions on making the access mode selection.
- Health status – Health status shows **ok** for servers with no problems, and either **warning** or **error** for servers with problems. Click the server name to view details.
- Upgrade status – Upgrade status shows the status of any upgrades in process.
- % memory used – The amount of memory currently used by each server is shown as a percentage of total memory available.
- Endpoints tested/minute – The number of endpoints tested over the last 15 minutes or less.
- Endpoints queued – The number of tests running or scheduled to run on that ES.
- System load average – The number of processes waiting to run (`top` command). In Linux, entering `top` at the command line returns a real-time look at processor activity.

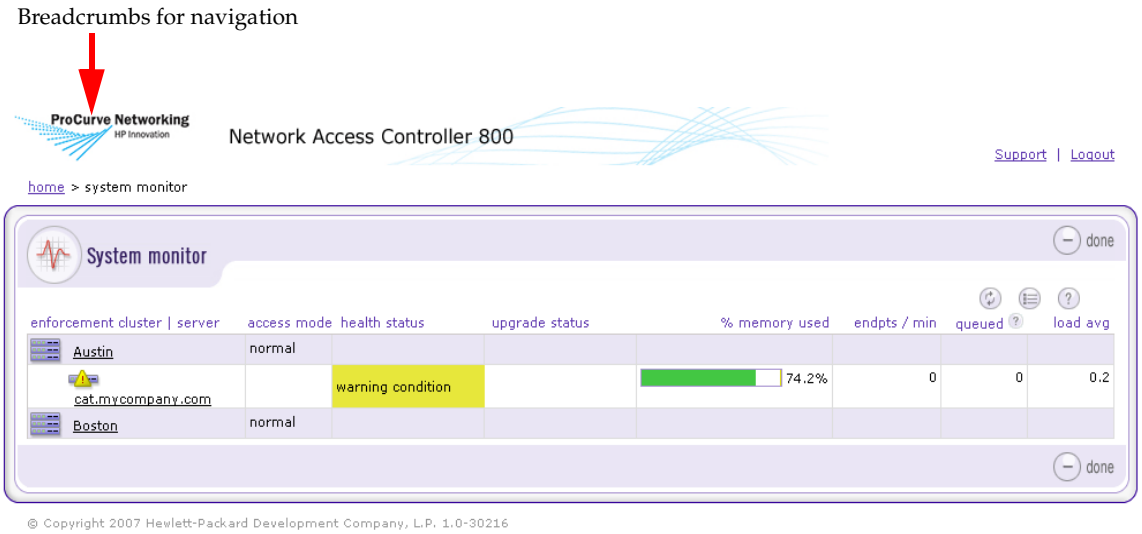


Figure 1-2. System Monitor Window

The following figure shows the legend for the System monitor window icons:

Enforcement clusters
cluster in normal mode
all servers in cluster have an error condition (unable to fail over)
cluster in failover mode
Enforcement server health
server is okay
server has error condition
server has warning condition
server is unavailable

Figure 1-3. System Monitor Window Legend

Overview

NAC 800 protects the network by ensuring that endpoints are free from threats and in compliance with the organization's IT security standards. NAC 800 systematically tests endpoints—with or without the use of a client or agent—for compliance with organizational security policies, quarantining non-compliant machines before they damage the network.

NAC 800 ensures that the applications and services running on endpoints (such as LAN, RAS, VPN, and WiFi endpoints) are up-to-date and free of worms, viruses, trojans, P2P and other potentially damaging software. It dramatically reduces the cost and effort of securing your network's weakest links—the endpoints your IT group might not adequately control.

There are advantages and disadvantages inherent with each of the test method technologies. Having a choice of testing solutions enables you to maximize the advantages and minimize the disadvantages.

TIP: Agentless testing uses an existing Windows service (RPC). ActiveX testing uses an ActiveX control. ProCurve agent testing installs an agent (ProCurve NAC EI Agent) and runs as a new Windows service.

The trade-offs in the test methods are described in the following table:

Test method	Trade-offs	
	Pros	**Cons**
Agentless	• Truly agentless, no install or download. • No extra memory load on the client machine. • Can begin testing, view test results, and give network access without any end-user interaction for endpoints on your Windows domains. • Easiest of the three test methods to deploy. • Saves administration time and is therefore less expensive than agent-based solutions.	• Requires RPC Service to be available to the NAC 800 server (ports 139 or 445). • Requires file and print sharing to be enabled. • Not supported by legacy Windows™ operating systems and non-Windows operating systems. • If the endpoint is not on a domain, the user must specify local credentials. A user often does not know what credentials to enter.

Table 1-1.Test Methods

Test method	Trade-offs	
	Pros	**Cons**
ActiveX plug-in	• No installation or upgrade to maintain. • Supports all Windows operating systems. • Only Internet Explorer application access required through personal firewall. Must open port 1500.	• No retesting of endpoint once browser is closed. • Not supported by non-Windows operating systems. • Browser security settings must allow ActiveX control operation of signed and safe controls. This is the default for the Internet zone. Raise the Internet zone setting and make NAC 800 part of the trusted zone. • Requires interaction from end-users—they must download the control before they can access network.
ProCurve NAC EI Agent	• Always available for retesting. • The agent is automatically updated with product updates. • Supports all Windows platforms.	• Install and upgrade to maintain. • Requires one-time interaction from end-users—they must download and install before they can access network.

Table 1-1.Test Methods (cont.)

The following list highlights key features:

- Enforcement options – NAC 800 provides multiple enforcement options for quarantining endpoints that do not comply with your security policy (Inline, DHCP, and 802.1X). This enables NAC 800 to enforce compliance across complex, heterogeneous networks.
- High availability and load balancing – A multi-server NAC 800 deployment is mutually supporting. Should one server fail, other nodes within a cluster will automatically provide coverage for the affected network segment.

  Load balancing is achieved by an algorithm that spreads the endpoint testing load across all Enforcement servers in a cluster.
- Multiple-user, role-based access – In enterprise deployments numerous individuals, each with varying responsibilities, typically require access to information within NAC 800. Role-based access enables system administrators to control who has access to the data, the functions they are allowed to perform, and the information they can view and act on. Role-based access ensures the integrity of the enterprise-wide NAC 800 deployment and creates the separation of duties that conforms to security best-practices.

- Extensible – NAC 800's easy-to-use open API allows administrators to create custom tests for meeting unique organizational requirements. The API is fully exposed and thoroughly documented. Custom tests are created using scripts and can be seamlessly added to existing policies.
- Compatible with existing heterogeneous network infrastructure – No upgrades to your existing network infrastructure are required.
- Variety of enforcement options – Permit, deny, or quarantine based on test results.
- Self-remediation – Reduces IT administration by empowering users to bring their machines into compliance.
- Subscription-based licensing – Includes all test updates and software upgrades.

The NAC 800 Process

NAC 800 administrators create "NAC policies" that define which applications and services are permitted, and specify the actions to be taken when endpoints do not comply. NAC 800 automatically applies the NAC policies to endpoints as they log into the network, and periodically as the endpoints remain logged into the network. Based on results, endpoints are either permitted or quarantined to a specific part of the network, thus enforcing the organizational security standards. NAC 800 tracks all testing and connection activity and produces a range of reports for auditors, managers, and IT staff.

About NAC 800

NAC Policy Definition

NAC policies consist of individual tests that evaluate the security status of endpoints attempting to access the network. Specific tests assess operating systems, verify that key hotfixes and patches have been installed, ensure antivirus and other security applications are present and up-to-date, detect the presence of worms, trojans, and viruses, and check for potentially dangerous applications such as file sharing, peer-to-peer (P2P), or spyware. See "Tests Help" on page A-1 for more information.

Key features include:

- Out-of-the-box NAC policies – High, medium, and low security are ready to use with no additional configuration required.
- Standard tests – NAC 800 comes with a broad range of tests.

- Automatic test updates – NAC 800 is automatically updated with tests that cover newly released patches, hotfixes, software updates, worms, and trojans, and recommended security settings for common applications. New tests are automatically added to the test database as frequently as hourly, ensuring immediate protection against newly discovered threats.
- Organization-specific policies – Any number of NAC policies can be created and tailored to your organizational needs. Create policies for like endpoints (for example, all Windows 2000 workstations), for an IP range or specific IPs, or by geographic location.

Endpoint Testing

NAC 800 automatically tests all endpoints attempting to access your network through a LAN, RAS, VPN, or WiFi connection. Tests are fast and you are kept informed of test progress and results. After the initial compliance tests, NAC 800 periodically tests endpoints that have been granted access to ensure that real-time system changes do not violate the NAC policy.

TIP: NAC 800 passes approximately 9 to 16 kilobytes of total data between a single endpoint and a single NAC 800 server for a single testing session with the High Security NAC policy (approximately 20 tests). It typically takes between 5 and 10 seconds to all tests in a policy on a 100Mb LAN. If your endpoints are taking longer to test, there might be a configuration problem with DNS on the NAC 800 server.

NOTE: If the end-user selects ActiveX test and then closes the browser, their endpoint is not retested until the end-user opens another browser session, reloading the ActiveX agent.

Key features include:

- Multiple test method options – Agentless, ActiveX, or ProCurve NAC EI Agent. Select the most appropriate method for your environment or endpoint.
- Rapid testing and robust endpoint management – Thousands of endpoints can be tested and managed simultaneously.
- Continual testing – Endpoints are retested on an administrator-defined interval as long as they remain connected to the network.

Compliance Enforcement

Based on endpoint test results, NAC 800 takes the appropriate action. Endpoints that test compliant with the applied policy are permitted access. Non-compliant endpoints are either quarantined, or are given access for a temporary period. Implement the necessary fixes during this period.

Key features include:

- Flexible enforcement options – Grant or quarantine access criteria is designated by the administrator and driven by the criticality of selected tests and corporate security standards.
- Manual overrides – Administrators can retest, quarantine, or grant access to endpoints on demand.
- User notifications – Users of non-compliant endpoints receive immediate notification about the location of the endpoint deficiencies, as well as step-by-step information about implementing the corrections to achieve compliance.
- Administrator notifications – Administrators receive a variety of notifications and alerts based on testing and access activity.
- Graduated enforcement – Allows controlled system rollout.

Automated and Manual Repair

- Self-remediation – End-users are notified of where their endpoints are deficient and provided with remediation instructions.
- Access "grace period" – Non-compliant endpoints are granted access for a temporary, administrator-defined period to facilitate remediation.

Targeted Reporting

NAC 800 reports provide concise security status information on endpoint compliance and access activity. Specific reports are available for auditors, managers, and IT staff members.

For more information, see “Reports” on page 12-1.

Technical Support

Technical support is available through www.procurve.com.

Additional Documentation

NAC 800 documentation is available in a number of media formats and is accessible in a variety of ways:

- Quick-start card – The Quick-start card provides a high-level overview of the physical deployment options, software installation, post-installation configuration, the Users' Guide, and how to get support.
- Online help – Online help is an essential component that assists in the installation, configuration, and ongoing management of NAC 800. You can access the online help by clicking the question mark displayed in the upper-right corner of the primary interface elements.

Upgrading

Upgrading is described in“Checking for NAC 800 Upgrades” on page 3-27.

CAUTION:

Installing third-party software on the NAC 800 server is not supported. If you install additional software on the NAC 800 server, you need to remove it in order to troubleshoot any NAC 800 issues, and it will likely be partially or fully overwritten during NAC 800 release upgrades or patch installs, compromising the third-party software functionality. Additionally, installing third-party software and/or modifying the NAC 800 software can violate your license agreement.

Conventions Used in This Document

The conventions used in this document are described in this section:

Navigation Paragraph

Navigation paragraphs provide a quick visual on how to get to the screen or area discussed.

Example:

NAC 800 main window>>Configure system

Tip Paragraph

Tips provide helpful, but not required information.

Example:

TIP: Hover the cursor over the “x dhcp servers with errors” text to get additional information in a pop-up window.

Note Paragraph

Notes notify you of important information.

Example:

NOTE: If there is no activity for 30 minutes, the configuration window times out and you must log in again.

Caution Paragraph

Cautions notify you of conditions that can cause errors or unexpected results.

Example:

CAUTION: Do not rename the files or they will not be seen by NAC 800.

Warning Paragraph

Warnings notify you of conditions that can lock your system or cause damage to your data.

Example:

WARNING: Do not log in using SSH—this kills your session and causes your session to hang.

Bold Font

Bold font indicates the text that appears on a window or screen.

Example:

9. If the **Domains** connection method is enabled (**Credentials** tab, **enabled** check box), you must specify your Windows domain controller here.

Task Paragraph

Task paragraphs summarize the instructions that follow.

Example:

To enter LDAP information:

Italic Text

Italic text is used in the following cases:

- Showing emphasis –

  Low – You are not protected from potentially unsafe macros. (*Not recommended*).
- Indicating document titles –

  NAC 800 Installation Guide
- Indicating a variable entry in a command –

  `https://<IP_address>/index.html`

  In this case, you must replace <*IP_address*> with the actual IP address, such as `10.0.16.99`. Do not type the angled brackets.

Courier Font

Courier font is used in the following cases:

- Indicating path names –

  Change the working directory to the following:

  `C:\Program Files\<MyCompany>\ProCurve NAC EI Agent`

- Indicating text; enter exactly as shown –

  Enter the following URL in the browser address field:

  `https://<IP_address>/index.html`

  In this case, you must replace <*IP_address*> with the actual IP address, such as `10.0.16.99`. Do not type the angled brackets.

- Indicating file names –

  `SAIASConnector.ini`

Angled Brackets

Angled brackets enclose variable text that needs to be replaced with your specific values.

Example:

`https://<IP_address>/index.html`

In this case, you must replace <*IP_address*> with the actual IP address, such as `10.0.16.99`. Do not type the angled brackets.

Square Brackets

Square brackets are used in the following cases:

- Indicating keys to press on the keyboard –

  `[Ctrl]+[Shift]+[r]`

- Indicating a variable section in a *.INI file –

```
[Global]
NASList=192.168.200.135
```

- Indicating a list in a properties file –

```
Compliance.ObjectManager.DHCPConnec-
torServers=[192.168.51.130, 192.168.99.1]
```

Terms

Terms are defined in the “Glossary” on page D-1.

Example:

MAC Media Access Control – The unique number that identifies a physical endpoint. Generally referred to as the MAC address.

Copying Files

Whenever you copy a file from one machine to another, copy it using a secure copy utility that uses the Secure Shell (SSH) protocol. The exact syntax of the copy command will vary based on the utility you use.

Example:

10. Copy the `/usr/local/nac/properties/NACAVPs.txt` file from the NAC 800 server to the ACS server using PSCP (or other secure copy utility).

SCP

`scp` is a Linux/UNIX command used to copy files between Linux/UNIX machines. It has the following syntax:

```
scp user@source:/directory/file user@destination:/direc-
tory/file
```

`scp` is included with Linux/UNIX.

PSCP

`pscp` is a program used to copy files between Windows and Linux/UNIX machines.

To use `pscp`, you must first save it from the following location to the Windows machine:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Next, open a DOS (command) window on the Windows machine, and enter the commands as follows:

To copy a file from a Linux machine to a Windows machine, enter the following:

<pscp directory>`\pscp fred@example.com:/etc/hosts c:\temp\example-hosts.txt`

You will be prompted to enter a password for the Linux/UNIX machine.

To copy a file from a Windows machine to a Linux machine, enter the following:

<pscp directory>`\pscp c:\documents\foo.txt fred@example.com:/tmp/foo`

You will be prompted to enter a password for the Linux/UNIX machine.

NOTE: You can either enter the path to the PSCP.EXE file as part of the command, or cd to the directory where you saved the PSCP.EXE file before entering the pscp command.

(This page intentionally left blank.)

2

Clusters and Servers

Chapter Contents

Overview 2-2
Installation Examples 2-3

Overview

NAC 800 uses clusters and servers. A "cluster" is a logical grouping of one or more Enforcement servers (ESs) that are managed by one Management server (MS).

A single-server installation is one where the MS and ES are on one server. The ES is assigned to a Default cluster. This configuration is illustrated in figure 2-1.

A multiple-server installation is one where the MS is on one server and there are one or more ESs on separate servers. Each ES must be assigned to a cluster. This configuration is illustrated in figure 2-2.

The responsibilities of the MS and ES are as follows:

- Management server
  - Configuration
  - NAC policies
  - Quarantining
  - Endpoint activity
  - License
  - Test updates
- Enforcement server
  - Testing
  - Access control

The quarantine method is defined per cluster; all of the Enforcement servers in a given cluster use the same quarantine method (Inline, DHCP, or 802.1X). When using multiple clusters, each cluster can have a different quarantine method. Clusters cooperate to test and control access to the network, although the ESs in each cluster are not able to communicate with any ES in any other cluster.

Installation Examples

Single-server Installation

The simplest installation is where the MS and ES are installed on the same physical server as shown in the following figure:

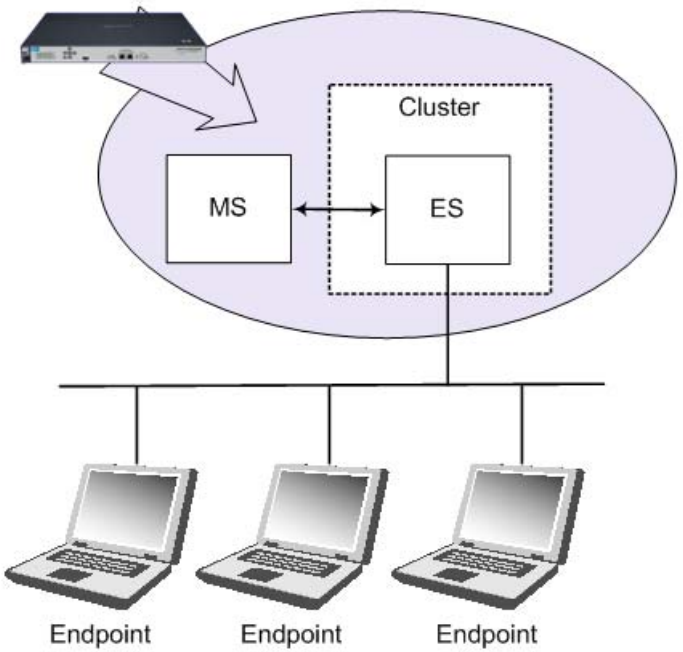


Figure 2-1. Single-server Installation

Multiple-server Installations

By using at least three servers, one for the MS and two for Enforcement servers, you gain the advantage of high availability and load balancing.

High availability is where Enforcement servers take over for any other Enforcement server or servers that become unavailable. Load balancing is where the testing of endpoints is spread evenly over all of the Enforcement servers. A three-server installation is shown in the following figure:

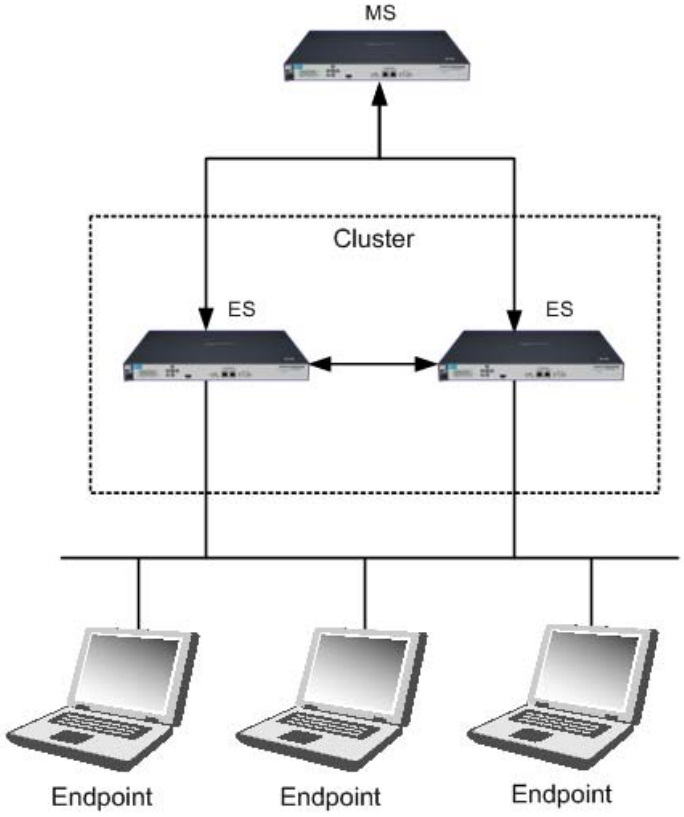


Figure 2-2. Multiple-server Installation

When your network is more complex, you can continue to add clusters as shown in the following figure:

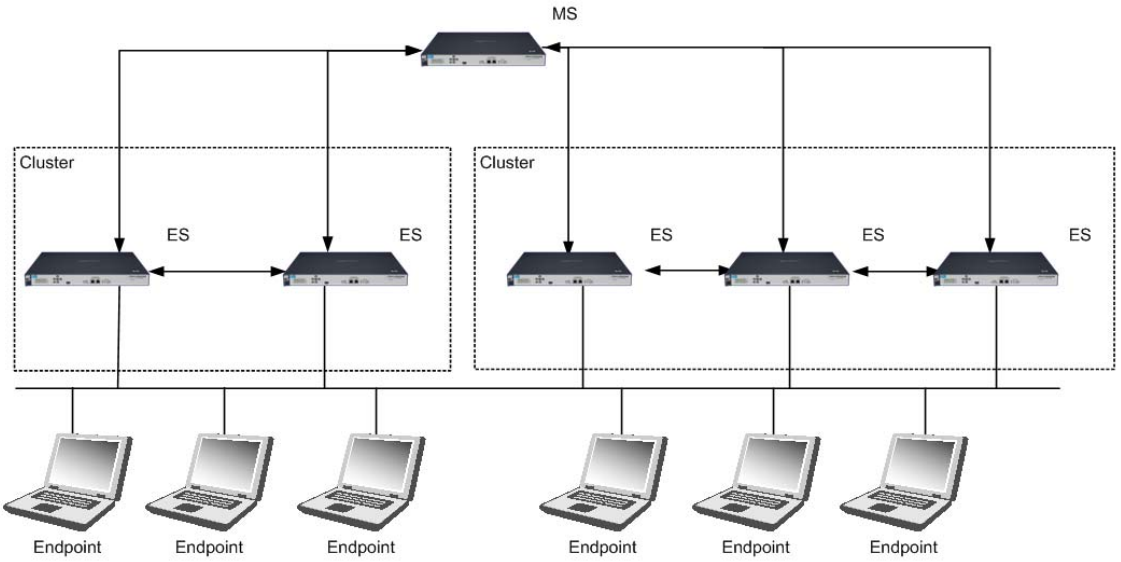


Figure 2-3. Multiple-server, Multiple-cluster Installation

The system configuration area allows you to select default settings for all clusters, as well as override the default settings on a per-cluster basis. See "System Configuration" on page 3-1 for task-based instructions.

The following recommendations should be followed when configuring your network for best performance results:

- A maximum of five ESs per cluster
- A maximum of 10 ESs per MS
- A maximum of 3000 endpoints per ES

When these recommendations are followed, the following applies:

- 80% of the 3000 endpoints will be tested in 30 seconds or less
- All endpoints are returned to the proper status within 15 minutes after a network recovery (power failure, all endpoints attempting to reconnect, 3000 endpoints per ES)

(This page intentionally left blank.)

3

System Configuration

Chapter Contents

Introduction 3-4
Enforcement Clusters and Servers 3-6
Enforcement Clusters 3-7
- Adding an Enforcement Cluster 3-7
- Editing Enforcement Clusters 3-9
- Viewing Enforcement Cluster Status 3-10
- Deleting Enforcement Clusters 3-11

Enforcement Servers 3-13
- Adding an Enforcement Server 3-13
- Cluster and Server Icons 3-15
- Changing the Enforcement Server Network Settings 3-17
- Changing the Enforcement Server Date and Time 3-17
- Modifying the ES root Account Password 3-18
- Modifying the ES root Account Password 3-18
- Viewing Enforcement Server Status 3-18
- Deleting Enforcement Servers 3-20
- Deleting Enforcement Servers 3-20
- Enforcement Server Recovery 3-20

Management Server 3-21
- Viewing Network Settings 3-21
- Modifying Management Server Network Settings 3-23
- Selecting a Proxy Server 3-23
- Setting the Date and Time 3-24
- Automatically Setting the Time 3-25
- Manually Setting the Time 3-25
- Selecting the Time Zone 3-26
- Changing MS SNMP Settings 3-26
- Modifying the MS root Account Password 3-26
- Checking for NAC 800 Upgrades 3-27

User Accounts 3-29
- Adding a User Account 3-29
- Searching for a User Account 3-32

Sorting the User Account Area 3-33
Copying a User Account 3-33
Editing a User Account 3-34
Deleting a User Account 3-35
User Roles 3-37
Adding a User Role 3-37
Editing User Roles 3-40
Deleting User Roles 3-41
Sorting the User Roles Area 3-42
License 3-43
Updating Your License 3-43
Test Updates 3-45
Manually Checking for Test Updates 3-45
Selecting Test Update Times 3-46
Viewing Test Update Logs 3-47
Quarantining 3-49
Selecting the Quarantine Method 3-49
Entering Basic 802.1X Settings 3-51
Selecting the RADIUS Authentication method 3-51
Configuring Windows Domain Settings 3-52
Configuring OpenLDAP Settings 3-54
Configuring Novell eDirectory Settings 3-57
Adding 802.1X Devices 3-60
Testing the Connection to a Device 3-61
Cisco IOS 3-62
Cisco CatOS 3-63
Enterasys 3-65
Extreme ExtremeWare 3-67
Extreme XOS 3-69
Foundry 3-71
HP ProCurve Switch 3-73
HP ProCurve WESM 3-76
HP ProCurve 420 AP or HP ProCurve 530 AP 3-79
Nortel 3-81
Other 3-83
Setting DHCP Enforcement 3-85
Adding a DHCP Quarantine Area 3-87
Sorting the DHCP Quarantine Area 3-89
Editing a DHCP Quarantine Area 3-89
Deleting a DHCP Quarantine Area 3-90

Maintenance 3-91
Initiating a New Backup 3-91
Restoring From a Backup 3-93
Downloading Support Packages 3-94
Cluster Setting Defaults 3-95
Testing Methods 3-95
Selecting End-user Options 3-98
Accessible Services 3-98
Exceptions 3-100
Notifications 3-102
End-user Screens 3-104
Agentless Credentials 3-107
Logging 3-111
Setting ES Logging Levels 3-111
Setting 802.1X Devices Logging Levels 3-112
Setting IDM Logging Levels 3-112
Advanced Settings 3-114
Setting the Agent Read Timeout 3-114
Setting the RPC Connection Timeout 3-114
Setting the RPC Command Timeout 3-115

Introduction

User logins and associated user roles determine the access permissions for specific functionality within NAC 800. The following table shows the default home window menu options that are available by user role:

User role	Home window menu options available
System Administrator	• Endpoint activity • NAC policies • System monitor • Reports • System configuration
Cluster Administrator	• Endpoint activity • System monitor • Reports • Enforcement clusters & servers
Help Desk Technician	• Endpoint activity • Reports
View-Only User	• Endpoint activity • Reports

Table 3-1.Default Menu Options

Only a system administrator can assign access permissions and access the **System configuration** window. See Figure 1-1 on page 1-5 for the NAC 800 home window of a user with system administration permissions. If you do not see the **System configuration** menu option, you do not have system administrator permissions.

NAC 800 configuration includes the following:

- Enforcement clusters & servers – "Enforcement Clusters and Servers" on page 3-6
- Management server – "Management Server" on page 3-21
- User accounts – "User Accounts" on page 3-29
- User roles – "User Roles" on page 3-37
- License – "License" on page 3-43
- Test updates – "Test Updates" on page 3-45

- Quarantining – "Quarantining" on page 3-49
- Maintenance – "Maintenance" on page 3-91
- Cluster setting defaults
  - Testing Methods – "Testing Methods" on page 3-95
  - Accessible services – "Accessible Services" on page 3-98
  - Exceptions – "Exceptions" on page 3-100
  - Notifications – "Notifications" on page 3-102
  - End-user screens – "End-user Screens" on page 3-104
  - Agentless credentials – "Agentless Credentials" on page 3-107
  - Logging – "Logging" on page 3-111
  - Advanced – "Advanced Settings" on page 3-114

NOTE: You can override any of the cluster default settings on a per-cluster basis.

Enforcement Clusters and Servers

The **Enforcement clusters & servers** menu option (figure 3-3) is where you configure Enforcement clusters and servers. You can perform the following tasks:

- Enforcement clusters
  - Add, edit, or delete Enforcement clusters
  - Set operating parameters for *specific* Enforcement clusters, which differ from the default Enforcement cluster and server settings set up on the **System configuration** window
  - View available Enforcement clusters and associated servers
  - View status of Enforcement clusters and servers
  - Select cluster access mode (normal, allow all, or quarantine all)
- Enforcement servers
  - Add, edit, or delete Enforcement servers
  - Set Enforcement server network settings, date and time, SNMP settings, and password
  - View available Enforcement servers
  - View status, memory usage, and disk space usage of Enforcement servers

Enforcement Clusters

Adding an Enforcement Cluster

To add an Enforcement cluster:

NAC 800 Home window>>System configuration>>Enforcement clusters & servers

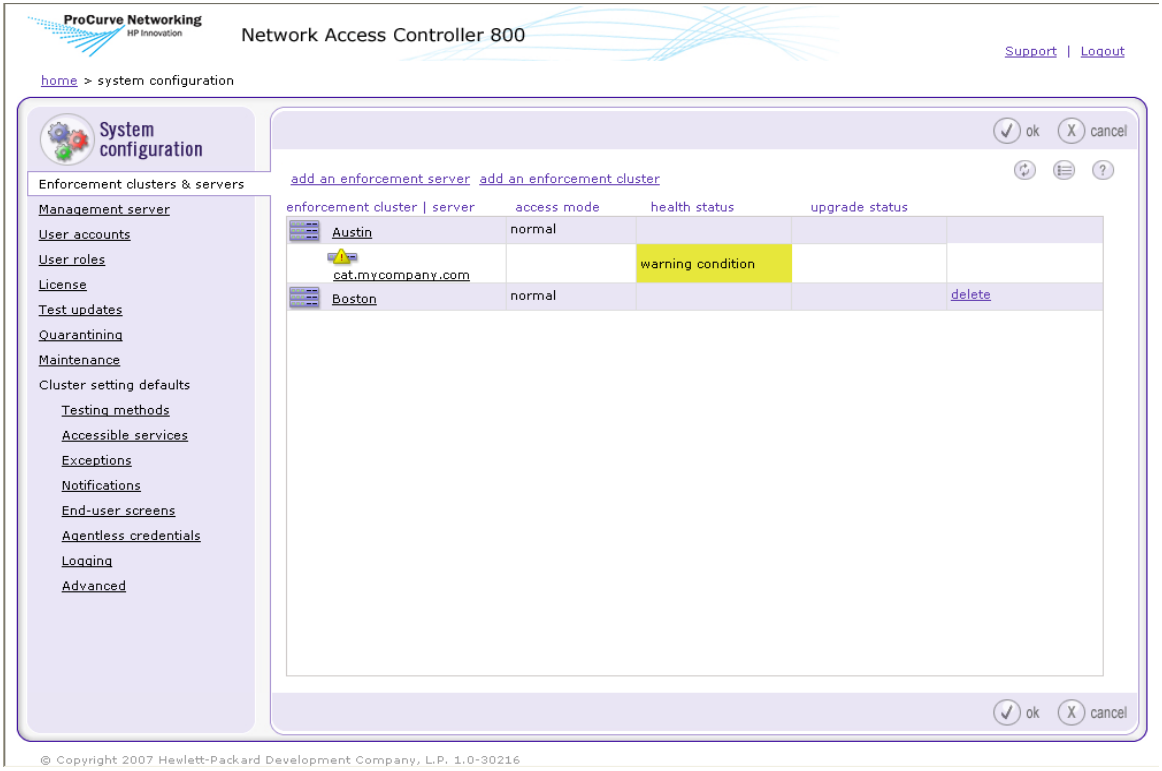


Figure 3-1. System Configuration Window, Enforcement Clusters & Servers Area

1. Click **Add an Enforcement cluster** in the **Enforcement clusters & servers** area. The **Add Enforcement cluster** window appears. The **General** area is displayed by default.

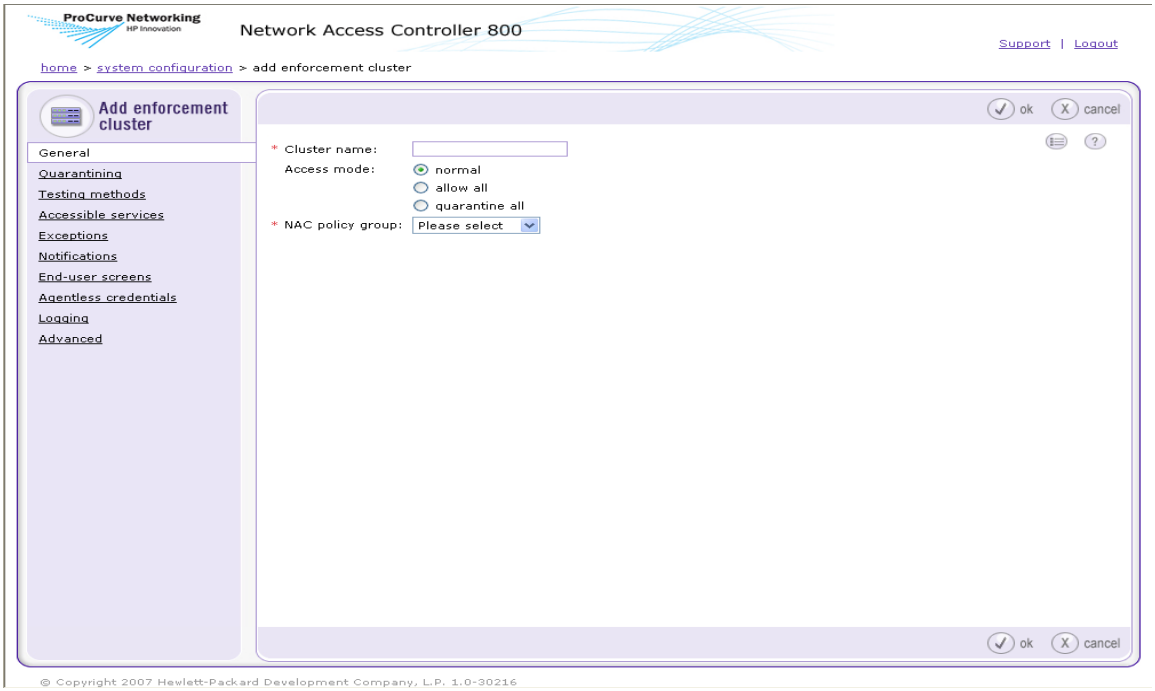


Figure 3-2. Add Enforcement Cluster Window

   a. Enter a name for the Enforcement cluster in the **Cluster name** field.
   b. Select one of the following access modes:
      – **normal** – Either allows or quarantines endpoints depending on the setup of the enforcement sever
      – **allow all** – Allows all endpoints
      – **quarantine all** – Quarantines all endpoints

NOTE: If you are setting up a cluster for the first time, and you have not yet added an ES, select **allow all** until you have finished configuring NAC 800.

   c. Select a NAC policy group from the **NAC policy group** drop-down list (see “NAC Policies” on page 6-1).

2. Click **Quarantining** in the **Add Enforcement cluster** window. Complete the steps described in “Quarantining” on page 3-49.

TIP: You can also access the quarantine area Enforcement cluster by clicking Quarantining in the System configuration window (see "Quarantining" on page 3-49 for more information).

3. The following cluster settings take on default values set from the **System configuration** window. To set up operating parameters that differ from those default settings, select the menu item of the settings you want to change, then select the **For this cluster, override the default settings** check box, and make the desired changes. Refer to the sections listed below to set up the default values, or for more information on the specific settings.
   - **Testing methods** – See "Testing Methods" on page 3-95
   - **Accessible services** – See "Accessible Services" on page 3-98
   - **Exceptions** – See "Exceptions" on page 3-100
   - **Notifications** – See "Notifications" on page 3-102
   - **End-user screens** – See "End-user Screens" on page 3-104
   - **Agentless credentials** – See "Agentless Credentials" on page 3-107
   - **Logging** – See "Logging" on page 3-111
   - **Advanced** – See "Advanced Settings" on page 3-114

Editing Enforcement Clusters

To edit the Enforcement clusters settings:

NAC 800 Home window>>System configuration>>Enforcement clusters & servers

1. Click the cluster you want to edit. The **Enforcement cluster** window appears, as shown in Figure 3-3 on page 3-11.
2. Click a menu option to access the cluster settings:
   - **General**
   - **Quarantining**
   - **Testing methods**
   - **Accessible services**
   - **Exceptions**
   - **Notifications**
   - **End-user screens**
   - **Agentless credentials**
   - **Logging**

- **Advanced**

3. Enter or change information in the fields you want to modify, as described in “Adding an Enforcement Cluster” on page 3-7.
4. Click **ok**.

Viewing Enforcement Cluster Status

There are two ways NAC 800 provides Enforcement cluster status:

- The icons next to the cluster name (see Figure 3-4 on page 3-13)
- The **Enforcement cluster** window (see the following steps)

To view Enforcement cluster statistics:

NAC 800 Home window>>System configuration>>Enforcement clusters & servers

Click a cluster name, for example Austin. The **Enforcement cluster** window appears:

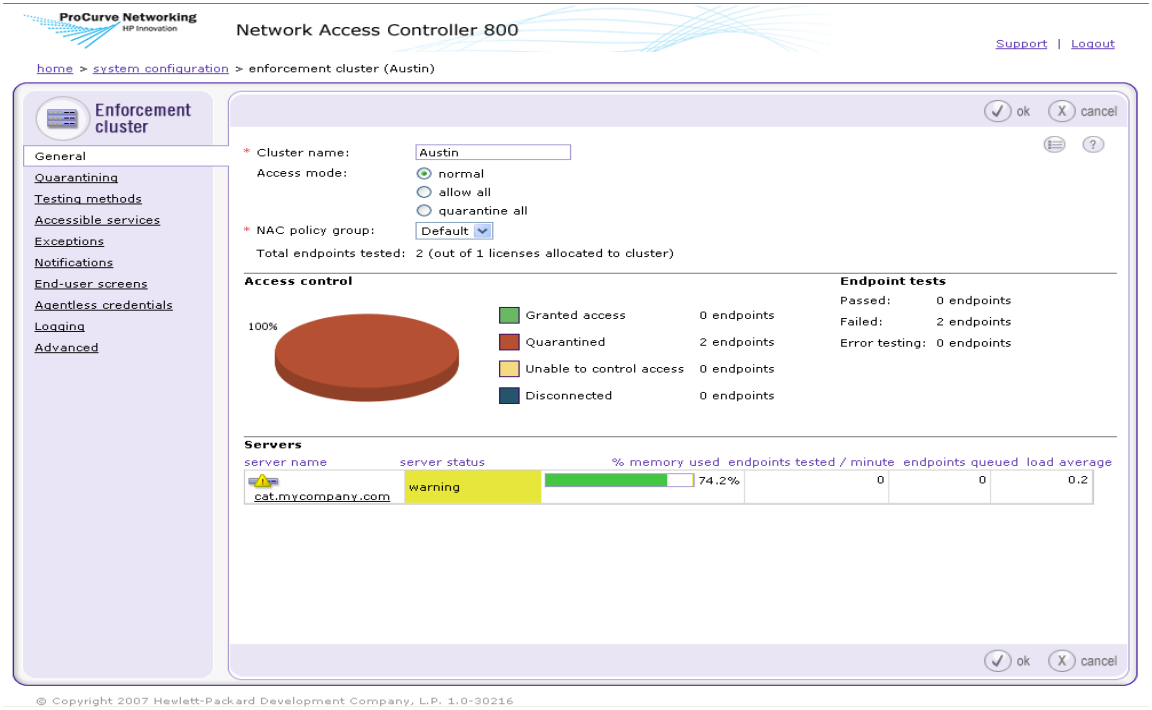


Figure 3-3. Enforcement Cluster Window, General Option

The statistics shown in this window are per cluster, where the statistics shown in the **Home** window are system-wide.

Deleting Enforcement Clusters

NOTE: Enforcement clusters need to be empty before the delete option appears next to the name in the NAC 800 console.

To delete Enforcement clusters:

NAC 800 Home window>>System configuration>>Enforcement clusters & servers

1. Click **delete** next to the cluster you want to remove. The **Delete Enforcement cluster** confirmation window appears.
2. Click **yes**. The **System configuration** window appears (figure 3-1).

Enforcement Servers

Adding an Enforcement Server

To add an Enforcement server:

NAC 800 home window>>System configuration>>Enforcement clusters & servers

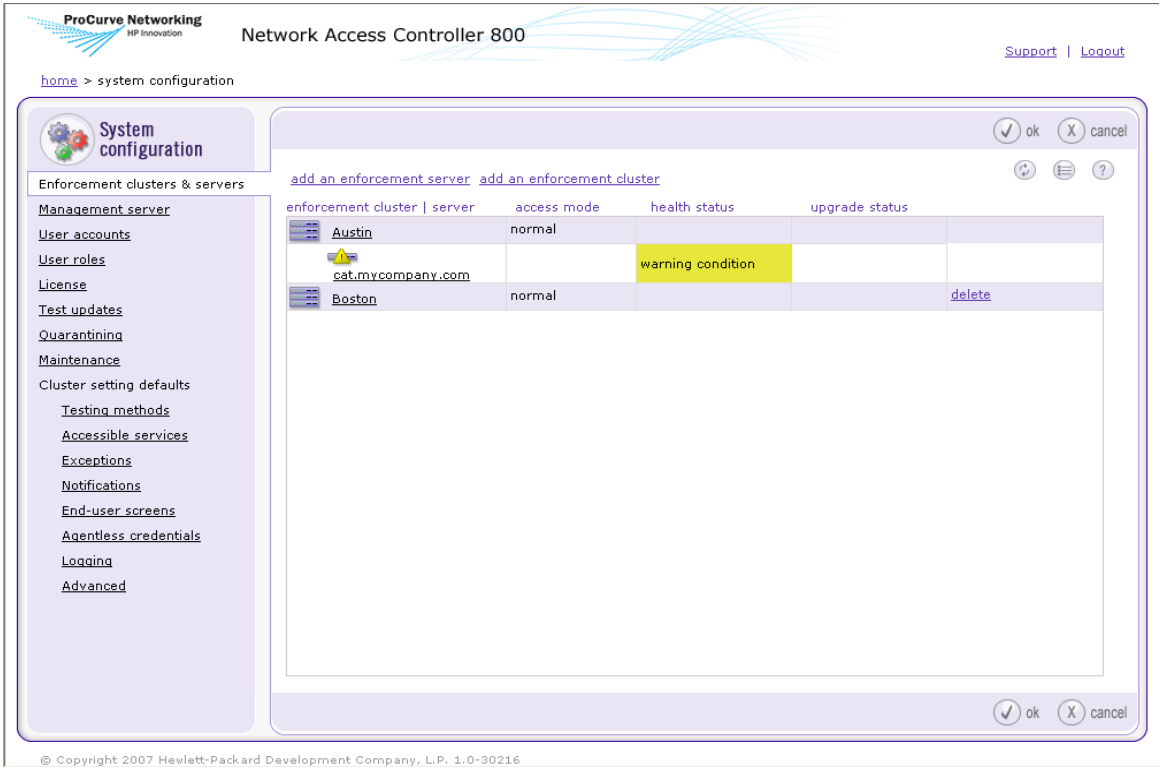


Figure 3-4. System Configuration Window, Enforcement Clusters & Servers Area

1. Click **Add an Enforcement server** in the **Enforcement clusters & servers** area. The **Add Enforcement server** window appears.

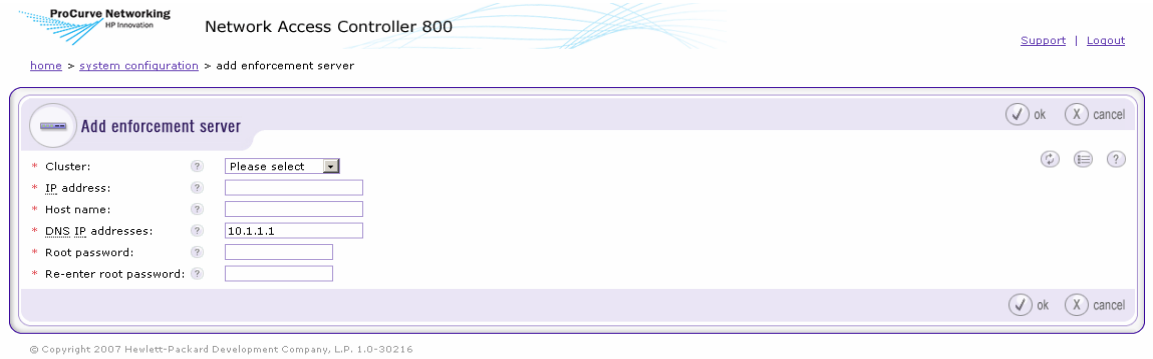


Figure 3-5. Add Enforcement Server Window

2. Select a cluster from the **Cluster** drop-down list.
3. Enter the IP address for this Enforcement server in the **IP address** text box.
4. Enter the fully qualified hostname to set on this server in the **Host name** text box.
5. Enter one or more DNS resolver IP addresses, separated by a commas, semicolons, or spaces in the **DNS IP addresses** text box. For example, `10.0.16.100,10.0.1.1`
6. Enter the password to set for the root user of the ES server's operating system in the **Root password** text box.
7. Re-enter the password to set for the root user of the ES server's operating system in the **Re-enter root password** text box.
8. Click **ok**.

Cluster and Server Icons

The following figure shows the legend explaining the Enforcement cluster and server status icons:

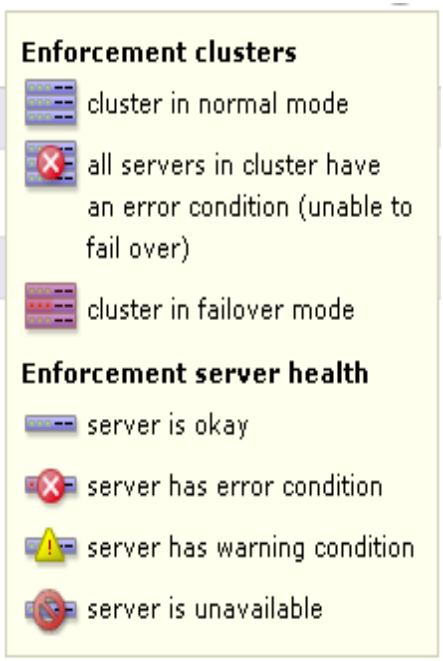

Enforcement clusters
cluster in normal mode
all servers in cluster have an error condition (unable to fail over)
cluster in failover mode
Enforcement server health
server is okay
server has error condition
server has warning condition
server is unavailable

Figure 3-6. Enforcement Cluster Legend

Editing Enforcement Servers

To edit Enforcement server settings:

NAC 800 Home window>>System configuration>>Enforcement clusters & servers

1. Click the Enforcement server you want to edit. The **Enforcement server** window appears, as shown in Figure 3-7 on page 3-16.

2. Click the **Configuration** menu option to access the Enforcement server's settings. The **Configuration** area is displayed:

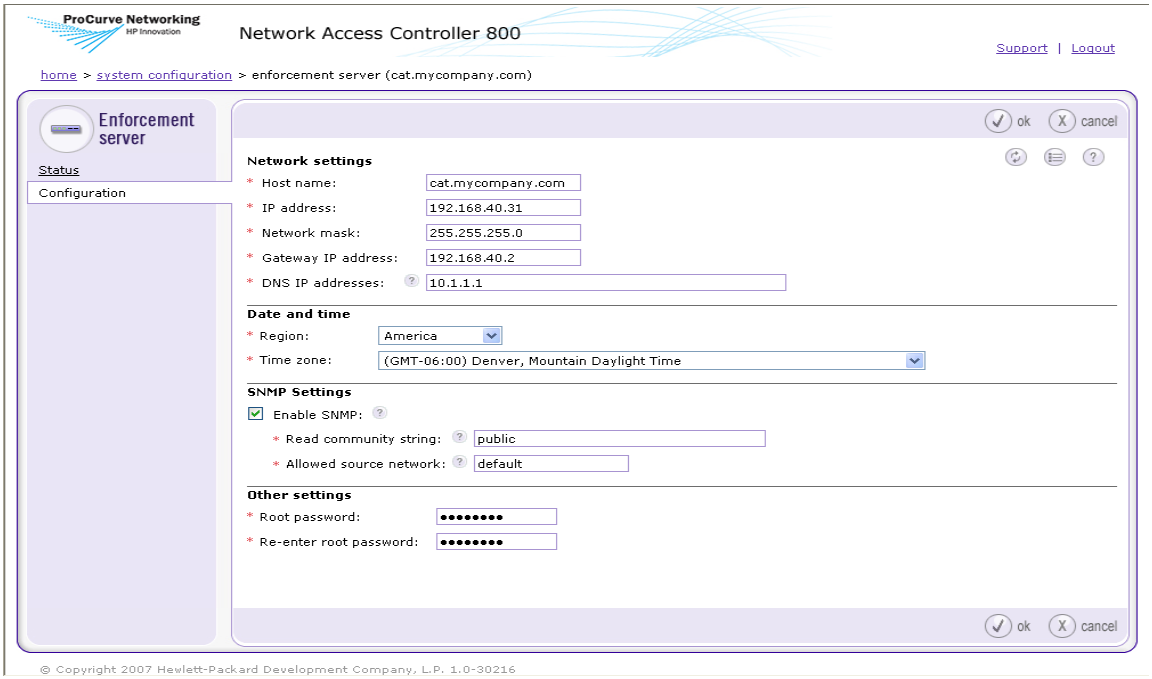


Figure 3-7. Enforcement Server Configuration Window

3. Edit the following setting(s):
   - Enforcement server network settings – "Changing the Enforcement Server Network Settings" on page 3-17
   - Enforcement server date and time – "Changing the Enforcement Server Date and Time" on page 3-17
   - Enforcement server SNMP settings – "Modifying the ES root Account Password" on page 3-18
   - Enforcement server password – "Modifying the ES root Account Password" on page 3-18
4. Click **ok**.

Changing the Enforcement Server Network Settings

CAUTION:

Back up your system immediately after changing the MS or ES IP address. If you do not back up with the new IP address, and later restore your system, it will restore the previous IP address which can show an ES error condition and cause authentication problems. See “Maintenance” on page 3-91 for instructions on backing up and restoring your system.

To change the Enforcement server network settings:

NAC 800 Home window>>System configuration>>Enforcement clusters & servers>>Select an ES>>Configuration

Modify any of the following **Network settings** you want to change:

- Enter a new Enforcement server in the **Host name** text field. For example, `garp.mycompany.com`
- Enter a new Enforcement server address in the **IP address** text field. For example, `192.168.153.35`
- Enter a new netmask in the **Network mask** text field. For example, `255.255.255.0`
- Enter a new gateway in the **Gateway IP address** text field. For example `192.168.153.2`
- Enter one or more DNS resolver IP addresses, separated by commas, semicolons, or spaces in the **DNS IP addresses** text box. For example: `10.0.16.100,10.0.1.1`

NOTE:

The NAC 800 Enforcement server’s host name must be a fully qualified domain name (FQDN). For example, the FQDN should include the host and the domain name—including the top-level domain.
For example, waldo.mycompany.com. Select names that are short, easy to remember, have no spaces or underscores, and the first and last character cannot be a dash (-).

NOTE:

You cannot change the ES IP address for a single-server installation. You can change the MS IP address for a single-server installation.

Changing the Enforcement Server Date and Time

To change the Enforcement server date and time:

NAC 800 Home window>>System configuration>>Enforcement clusters & servers>>Select an ES>>Configuration

1. Select a Region from the **Region** drop-down list in the **Date and time** area.
2. Select a time zone from the **Time zone** drop-down list.
3. Click **ok.**

NOTE: See "Selecting the Time Zone" on page 3-26 for information on changing the time zone settings for the Management server.

WARNING: Manually changing the date/time by a large amount (other than a time zone change) will require a restart of all servers. Rolling back the clock will have adverse effects on the system.

Modifying the ES root Account Password

To change the Enforcement server `root` account password:

NAC 800 Home window>>System configuration>>Enforcement clusters & servers>>Select an ES>>Configuration

1. Enter the new password in the **Root password** text box in the **Other settings** area.
2. Re-enter the password in the **Re-enter root password** text box.
3. Click **ok**.

Viewing Enforcement Server Status

There are two ways NAC 800 provides ES status:

- The icons next to the server name (see Figure 3-6 on page 3-15)
- The **Status** window (see the following steps). The **Enforcement server** window allows you to view the following information:
  - Health status
  - Upgrade status
  - Process/thread status
  - System load average for the server
  - Current endpoints being tested/minute for the server

- Percentage of memory used on the server
- Disk space usage for the server

To view Enforcement server status:

NAC 800 Home window>>System configuration>>Enforcement clusters & servers

1. Click the server for which you want to view the status. The **Enforcement server** window appears:

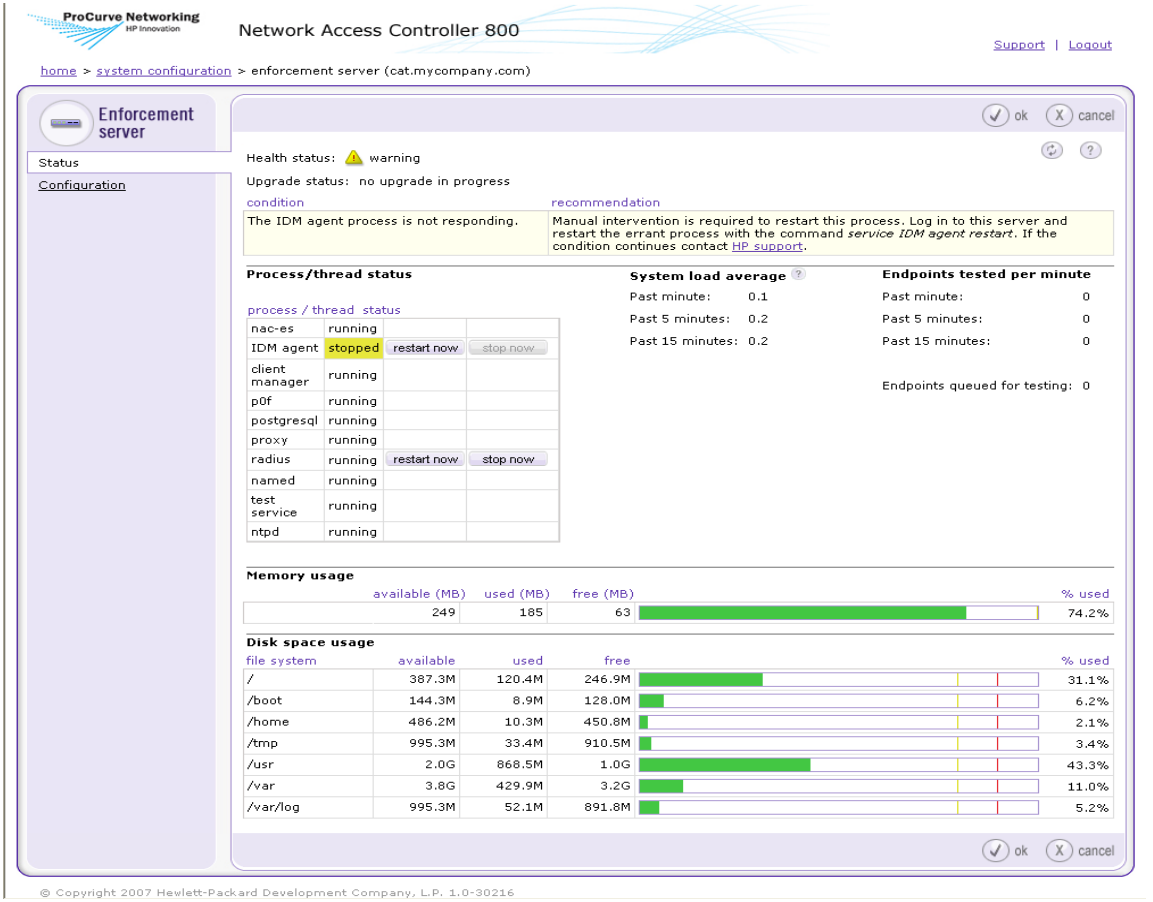

ProCurve Networking
HP Innovation
Network Access Controller 800
Support | Logout
home > system configuration > enforcement server (cat.mycompany.com)
Enforcement server
Status
Configuration
ok
cancel
Health status: warning
Upgrade status: no upgrade in progress
condition
recommendation
The IDM agent process is not responding.
Manual intervention is required to restart this process. Log in to this server and restart the errant process with the command service IDM agent restart. If the condition continues contact HP support.
Process/thread status
process / thread status
nac-es running
IDM agent stopped restart now stop now
client manager running
p0f running
postgresql running
proxy running
radius running restart now stop now
named running
test service running
ntpd running
System load average
Past minute: 0.1
Past 5 minutes: 0.2
Past 15 minutes: 0.2
Endpoints tested per minute
Past minute: 0
Past 5 minutes: 0
Past 15 minutes: 0
Endpoints queued for testing: 0
Memory usage
available (MB) used (MB) free (MB) % used
249 185 63 74.2%
Disk space usage
file system available used free % used
/ 387.3M 120.4M 246.9M 31.1%
/boot 144.3M 8.9M 128.0M 6.2%
/home 486.2M 10.3M 450.8M 2.1%
/tmp 995.3M 33.4M 910.5M 3.4%
/usr 2.0G 868.5M 1.0G 43.3%
/var 3.8G 429.9M 3.2G 11.0%
/var/log 995.3M 52.1M 891.8M 5.2%
ok
cancel
© Copyright 2007 Hewlett-Packard Development Company, L.P. 1.0-30216

Figure 3-8. Enforcement Server Window, Status Option

2. Click **ok** or **cancel**.

Deleting Enforcement Servers

NOTE: Servers need to be powered down for the delete option to appear next to the name in the NAC 800 console.

To delete Enforcement servers:

NAC 800 Home window>>System configuration>>Enforcement clusters & servers

1. Click **delete** next to the server you want to remove from the cluster. The **Delete Enforcement server** confirmation window appears.
2. Click **yes**. The **System configuration** window appears.

Enforcement Server Recovery

If an existing ES goes down and comes back up, it can participate in its assigned cluster, even if the MS is not available.

When a new ES is created, the MS must be available before the ES can participate in a cluster.

Management Server

Viewing Network Settings

To view Management servers status:

NAC 800 Home window>>System configuration>>Management server

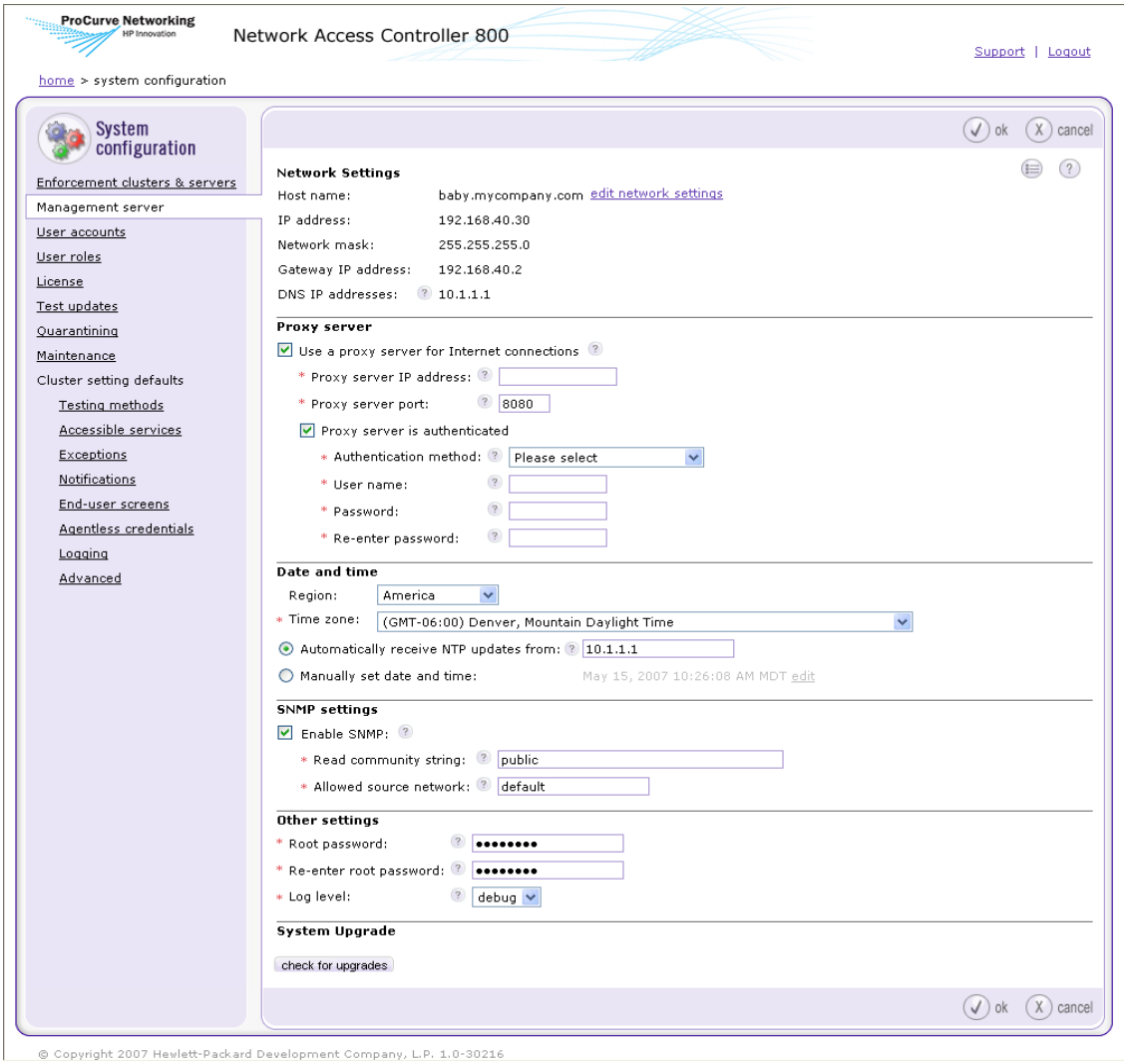


Figure 3-9. System Configuration, Management Server Window

1. Server status is shown in the Network settings area.
2. Click **ok** or **cancel**.

Modifying Management Server Network Settings

CAUTION:

Back up your system immediately after changing the MS or ES IP address. If you do not back up with the new IP address, and later restore your system, it will restore the previous IP address which can show an ES error condition and cause authentication problems. See “Maintenance” on page 3-91 for instructions on backing up and restoring your system.

To modify Management server network settings:

NAC 800 Home window>>System configuration>>Management server

WARNING:

Changing the Management server network settings will cause the network interface to restart.

1. Click **edit network settings** in the **Network settings** area.
2. Enter the values you want to modify:
   - Enter a new name in the **Host name** text field. For example, `garp.mycompany.com`

NOTE:

Select names that are short, easy to remember, have no spaces or underscores, and the first and last character cannot be a dash (-).

   - Enter a new address in the **IP address** text field. For example, `192.168.153.35`
   - Enter a new netmask in the **Network mask** text field. For example, `255.255.255.0`
   - Enter a new gateway in the **Gateway IP address** text field. For example `192.168.153.2`
   - Enter one or more DNS resolver IP addresses, separated by commas, semicolons, or spaces in the **DNS IP addresses** text box. For example: `10.0.16.100,10.0.1.1`
3. Click **ok**.

Selecting a Proxy Server

Connecting to the Internet is necessary for updating tests, validating license keys, and sending support packages.

To select a proxy server:

NAC 800 Home window>>System configuration>>Management server

1. Select **Use a proxy server for Internet connections**.
2. Enter the IP address of the server that will act as the proxy for Internet connections in the **Proxy server IP address** text field.
3. Enter the port used for connecting to the proxy server in the **Proxy server port** text field.
4. If your proxy server requires authentication, select the **Proxy server is authenticated** check box.
   a. **Authentication method** – Select the scheme used to authenticate credentials on the proxy server. The following methods are supported:
      – **Basic (not recommended)** – The original and most compatible authentication scheme for HTTP. Also the least secure because it sends the user ID and password to the server unencrypted.
      – **Digest** – Added in the HTTP 1.1 protocol, this scheme is significantly more secure than basic authentication because it never transfers the actual password across the network, but instead uses it to encrypt a "nonce" value sent from the server.
      – **Negotiable** – Using this scheme, the client and the proxy server negotiate a scheme for authentication. Ultimately, either the basic or digest scheme will be used.
   b. Enter the ID of a user account on the proxy server in the **User name** text box.
   c. Enter the password of the user account specified in the **User name** text box in the **Password** text box.
   d. Re-enter the password.
5. Click **ok**.

Setting the Date and Time

The **Date and time** area allows you to configure the following:

- Allow automatic synchronization with an NTP server
- Manually set date and time for the Management server
- Edit date and time:
  - Set time zone
  - Set date

- Set time

NOTE: Date and time settings are applied to the MS; however, you can set the time zone for each ES.

Automatically Setting the Time

To automatically set the time:

NAC 800 Home window>>System configuration>>Management server

1. Select **Automatically receive NTP updates from** and enter one or more Network Time Protocol (NTP) servers, separated by commas. The NTP protocol allows NAC 800 to synchronize its date and time with other endpoints on your network. For example, `time.nist.gov`.
2. Click **ok**.

TIP: Use of NTP is strongly recommended.

Manually Setting the Time

To manually set the time:

NAC 800 Home window>>System configuration>>Management server

1. Select **Manually set date & time**.
2. Click **edit**. The **Date and time** window appears:

Figure 3-10. Date & Time Window

3. Select the correct date and time.
4. Click **ok**.
5. Click **ok**.

CAUTION:

Manually changing the date/time (other than a time zone change) a large amount will require a restart of all servers. Rolling back the clock will have adverse effects on the system.

Selecting the Time Zone

To set the time zone:

NAC 800 Home window>>System configuration>>Management server

1. Select the following:
   a. Select a region from the **Region** drop-down list in the **Date and time** area.
   b. Select a time zone from the **Time zone** drop-down list.
2. Click **ok**.

Changing MS SNMP Settings

To change the Management server SNMP settings:

NAC 800 Home window>>System configuration>>Management server

1. Select the **Enable SNMP** check box to enable SNMP. Clear the check box to disable SNMP. NAC 800 supports read-only SNMP v1 and v2.
2. Enter the **Read community string**. The default setting for network equipment is often set to `public`. To prevent network information from being divulged, change the community string to something unique.
3. Enter the SNMP **Allowed source network**. The value must be either `default` or a network specified in CIDR notation.
4. Click **ok**.

Modifying the MS root Account Password

To change the Management server `root` account password:

NAC 800 Home window>>System configuration>>Management server

1. Enter the new password in the **Root password** text box in the **Other settings** area.
2. Re-enter the password in the **Re-enter root password** text box.
3. Click **ok**.

Checking for NAC 800 Upgrades

To check for system upgrades:

NAC 800 Home window>>System configuration>>Management server

1. Click **check for upgrades** in the **System upgrade** area. A progress window appears.
2. A status window appears indicating if upgrades are available.
   a. If no upgrades are available, click **ok** to clear the status window.
   b. Click **ok** to return to **System configuration**.
   c. If an upgrade is available, click **yes** to upgrade your system.

CAUTION: Installation of an upgrade can take several hours to download all the software. You can continue to use NAC 800 during the download process. NAC 800 will automatically shutdown and restart after the software downloads.

TIP: Since upgrading can take longer than the default timeout setting of the NAC 800 Console, ProCurve recommends that you increase the timeout value when you have limited bandwidth by performing the steps described in "Changing the NAC 800 Console Timeout".

Changing the NAC 800 Console Timeout

To change the timeout value for the console:

Command window

1. Log in to the NAC 800 server as `root`, either using SSH or directly with a keyboard.

2. Enter the following at the command line:

   ```
   setProperty.py -m
   Compliance.UpgradeManager.UpgradeTimeout=<minutes>
   ```

   Where:

   <*minutes*> is the number of minutes of inactivity NAC 800 will wait before requiring the user to log in to the console again. For example,30.

User Accounts

NAC 800 allows you to create multiple user accounts. User accounts provide and limit access to NAC 800 functions based on permissions (user roles) and clusters assigned. See “User Roles” on page 3-37 for more information on setting permissions for the user roles.

The **User accounts** menu option allows you to do the following:

- View user accounts
- Search by user ID, user name, or email address
- Add a user account
- Edit a user account
- Delete a user account

Adding a User Account

To add a user account:

NAC 800 Home window>>System configuration>>User accounts

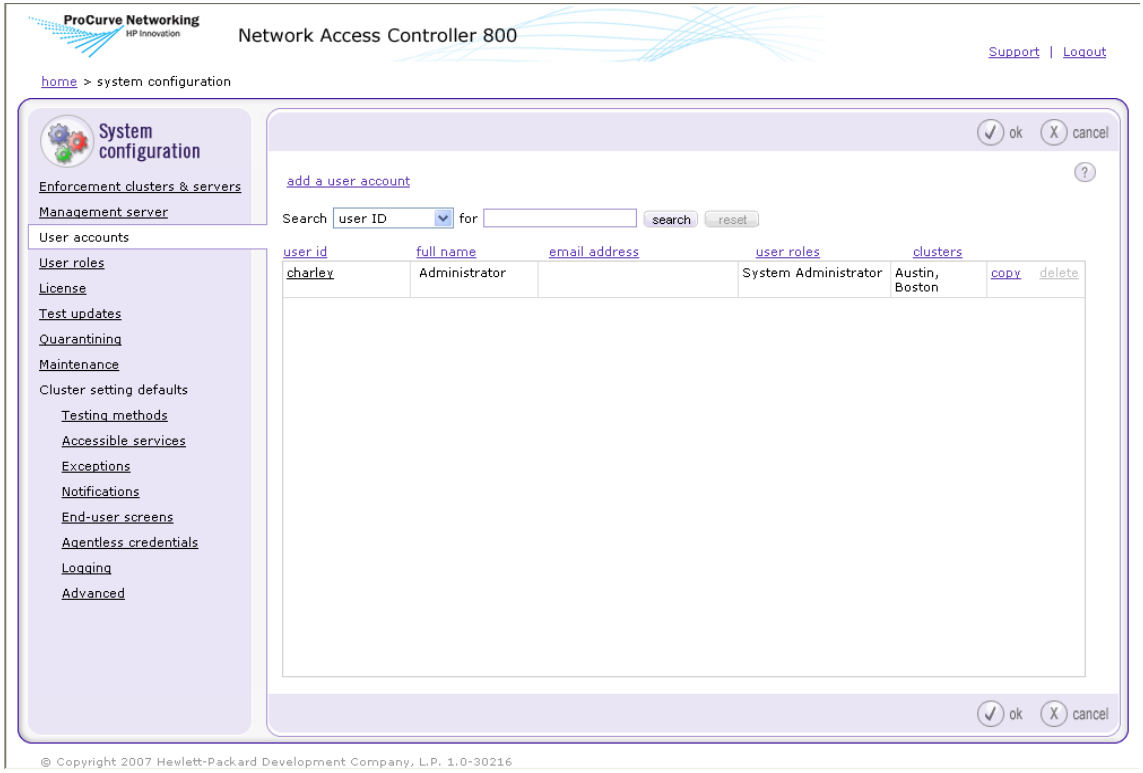


Figure 3-11. System Configuration, User Accounts

1. Click **Add a user account**. The **Add user account** window appears:

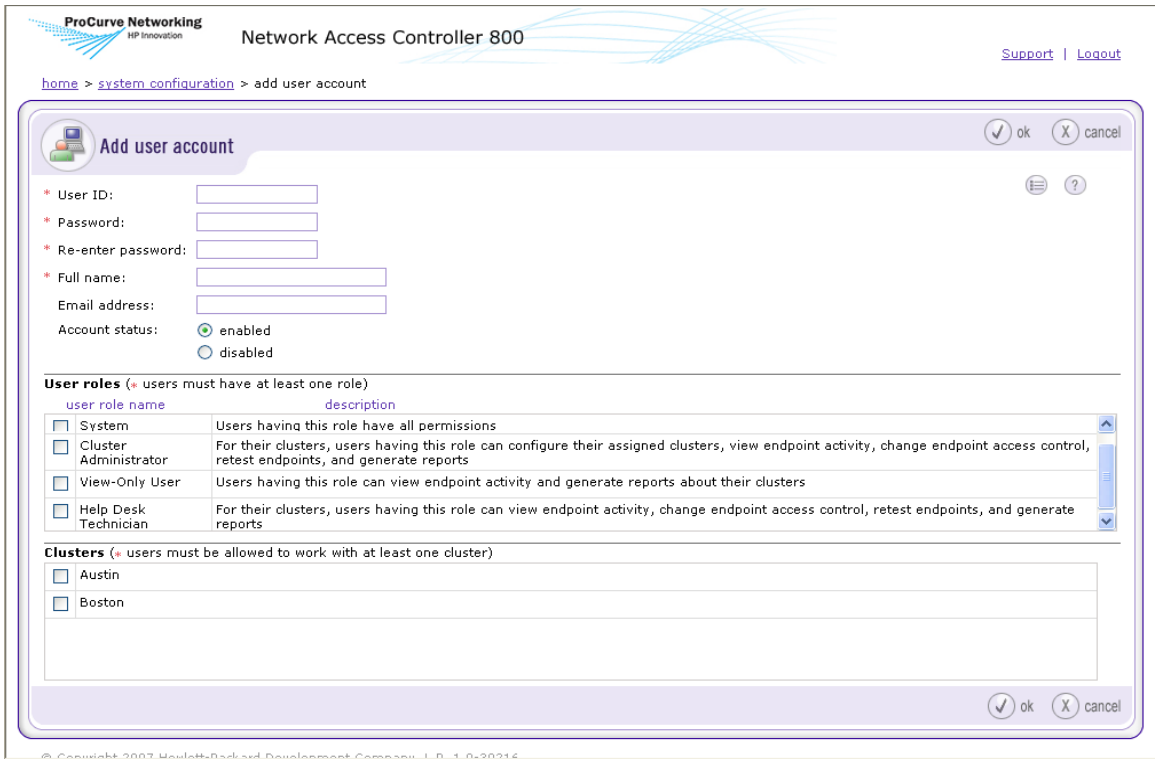

ProCurve Networking
HP Innovation
Network Access Controller 800
Support | Logout
home > system configuration > add user account
Add user account
ok
cancel
* User ID:
* Password:
* Re-enter password:
* Full name:
Email address:
Account status:
enabled
disabled
User roles (* users must have at least one role)
user role name
description
System
Users having this role have all permissions
Cluster Administrator
For their clusters, users having this role can configure their assigned clusters, view endpoint activity, change endpoint access control, retest endpoints, and generate reports
View-Only User
Users having this role can view endpoint activity and generate reports about their clusters
Help Desk Technician
For their clusters, users having this role can view endpoint activity, change endpoint access control, retest endpoints, and generate reports
Clusters (* users must be allowed to work with at least one cluster)
Austin
Boston
ok
cancel

Figure 3-12. Add User Account

2. Enter the following information:
   - **User ID** – The user ID used to log into NAC 800
   - **Password** – The password used to log into NAC 800
   - **Full name** – The name associated with the user account
   - **Email address** – The email address used for notifications
3. Select an Account status:
   - **enabled** – This status allows an account to log into the console
   - **disabled** – This status prevents an account from logging into the console
4. In the **User roles** area, select one of the following default roles for the user account: (See “User Roles” on page 3-37 for more information about user roles and permissions associated with user roles.)

- **Cluster Administrator**
- **View-Only User**
- **System Administrator**
- **Help Desk Technician**
- You can select a custom user role if you have created any.

NOTE: Users must be assigned at least one role.

5. In the **Clusters** area, select a cluster or clusters.

NOTE: Users must be assigned at least one Enforcement cluster.

User Role Name	Description
Cluster Administrator	For their clusters, users having this role can configure their assigned clusters, view endpoint activity, change endpoint access control, retest endpoints, and generate reports.
View-Only User	Users having this role can view endpoint activity and generate reports about their clusters.
System Administrator	Users having this role have all permissions.
Help Desk Technician	For their clusters, users having this role can view endpoint activity, change endpoint access control, retest endpoints, and run reports.
User-defined role	Create your own user roles and definitions.

Table 3-2.Default User Roles

6. Click **ok**.

Searching for a User Account

To search for a user account:

NAC 800 Home window>>System configuration>>User accounts

1. Select one of the following from the **Search** drop-down list:
   - **user ID**
   - **full name**
   - **email address**

2. Enter the text to search for in the **for** field.
3. Click **search**.

TIP: Click **reset** to clear the text field and to refresh the display to show all accounts after a search.

Sorting the User Account Area

To sort the user account area:

NAC 800 Home window>>System configuration>>User accounts

Click the column heading for **user id**, **full name**, **email address**, **user roles**, or **clusters**. The user accounts reorder according to the column heading selected. Click the column heading again to change from ascending to descending.

Copying a User Account

To copy a user account:

NAC 800 Home window>>System configuration>>User accounts

1. Click **copy** next to the user account you want to duplicate. The **Copy user account** window appears. The account information is duplicated from the original account.

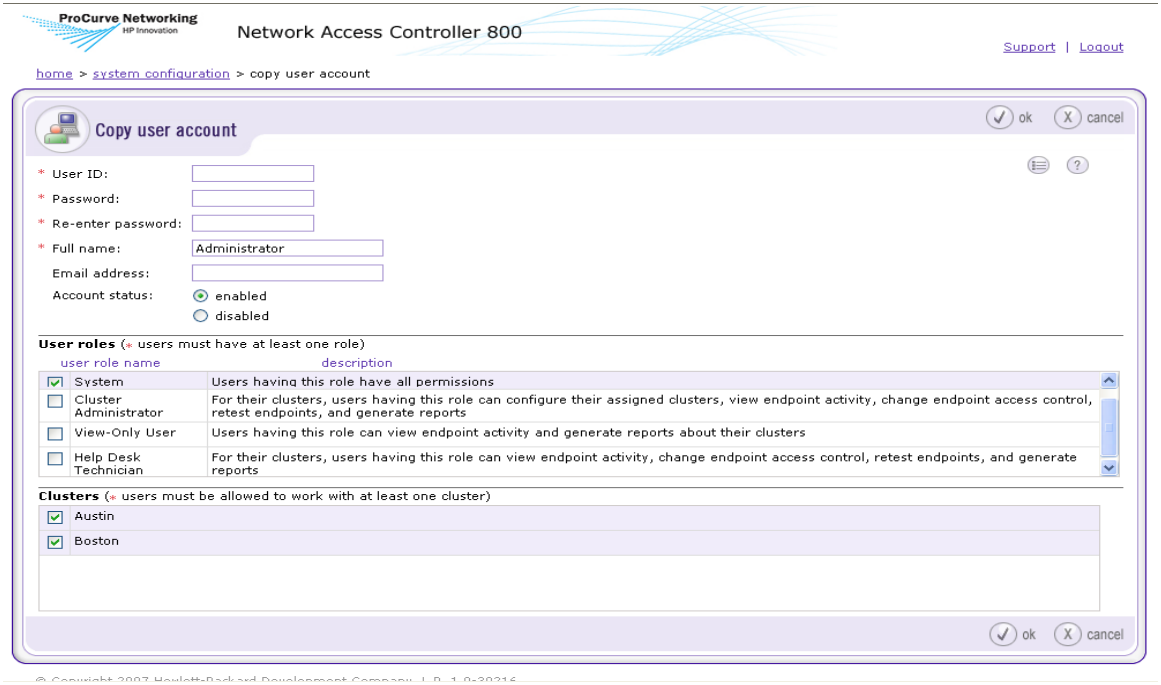

ProCurve Networking
HP Innovation
Network Access Controller 800
Support | Logout
home > system configuration > copy user account
Copy user account
ok
cancel
* User ID:
* Password:
* Re-enter password:
* Full name:
Administrator
Email address:
Account status:
enabled
disabled
User roles (* users must have at least one role)
user role name
description
System
Users having this role have all permissions
Cluster Administrator
For their clusters, users having this role can configure their assigned clusters, view endpoint activity, change endpoint access control, retest endpoints, and generate reports
View-Only User
Users having this role can view endpoint activity and generate reports about their clusters
Help Desk Technician
For their clusters, users having this role can view endpoint activity, change endpoint access control, retest endpoints, and generate reports
Clusters (* users must be allowed to work with at least one cluster)
Austin
Boston
ok
cancel

Figure 3-13. Copy User Account

2. Enter the **User ID** of the new account.
3. Enter the **Password**.
4. Re-enter the **password**.
5. Select the **Account status** (**enable** or **disable**).
6. Select the **User role** for the account.
7. Select the **Cluster(s)** that the user account can access.
8. Click **ok**.

Editing a User Account

To edit a user account:

NAC 800 Home window>>System configuration>>User accounts

1. Click the name of the user account that you want to edit. The **User account** window appears:

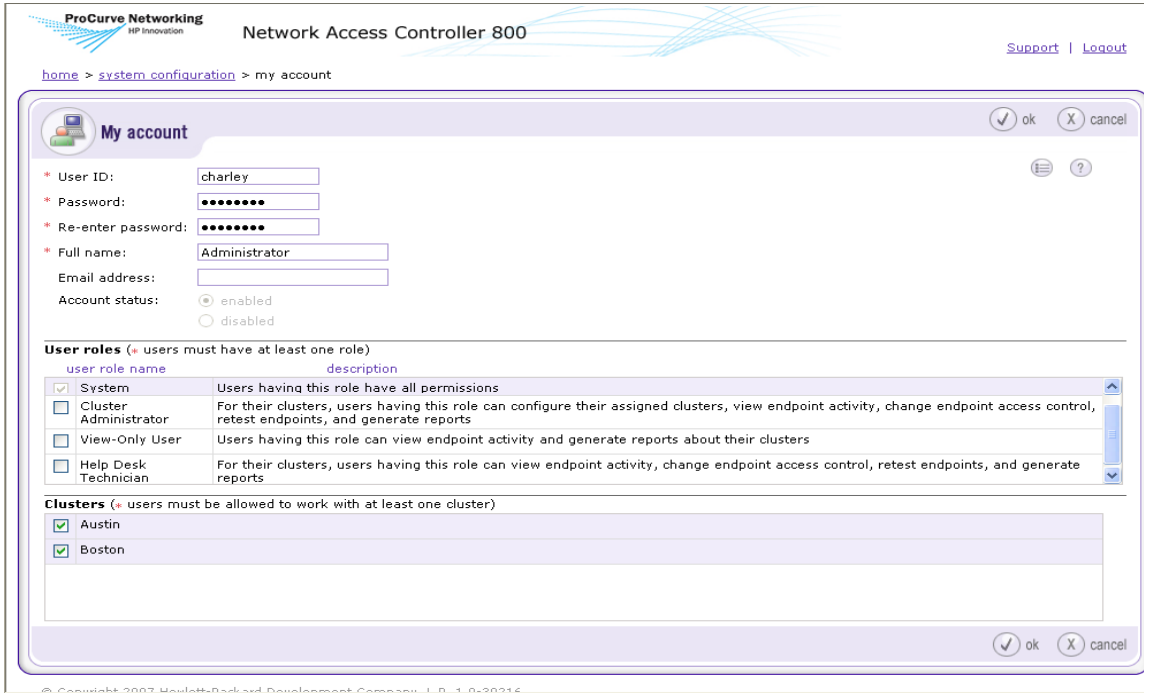

ProCurve Networking
HP Innovation
Network Access Controller 800
Support | Logout
home > system configuration > my account
My account
ok
cancel
* User ID: charley
* Password: ••••••••
* Re-enter password: ••••••••
* Full name: Administrator
Email address:
Account status: enabled disabled
User roles (* users must have at least one role)
user role name
description
System
Users having this role have all permissions
Cluster Administrator
For their clusters, users having this role can configure their assigned clusters, view endpoint activity, change endpoint access control, retest endpoints, and generate reports
View-Only User
Users having this role can view endpoint activity and generate reports about their clusters
Help Desk Technician
For their clusters, users having this role can view endpoint activity, change endpoint access control, retest endpoints, and generate reports
Clusters (* users must be allowed to work with at least one cluster)
Austin
Boston
ok
cancel

Figure 3-14. User Account

2. Change or enter information in the fields you want to change. See "Adding a User Account" on page 3-29 for information on user account settings.
3. Click **ok**.

Deleting a User Account

You must always have at least one account with System Administrator permissions.

CAUTION: Do not delete or edit the account with which you are currently accessing the interface. Doing so can produce an error and lock you out of the interface until your session has timed out.

To delete a user account:

NAC 800 Home window>>System configuration>>User accounts

1. Click **delete** next to the user account you want to remove. The **Delete user account** confirmation window appears.
2. Click **yes**.

User Roles

The **User roles** menu option allows you to configure the following:

- View current user roles and details associated with those roles
- Add a new user role
  - Name the new user role
  - Provide a detail description for the new user role
  - Assign permissions to the new user role
- Edit a user role
  - Edit the name of the user role
  - Edit the detail description of the user role
  - Edit the assigned permissions for the user role
- Delete a user role

Adding a User Role

To add a user role:

NAC 800 Home window>>System configuration>>User roles

Figure 3-15. System Configuration Window, User Roles

1. Click **add a user role** in the **User roles** area. The **Add user role** window appears.

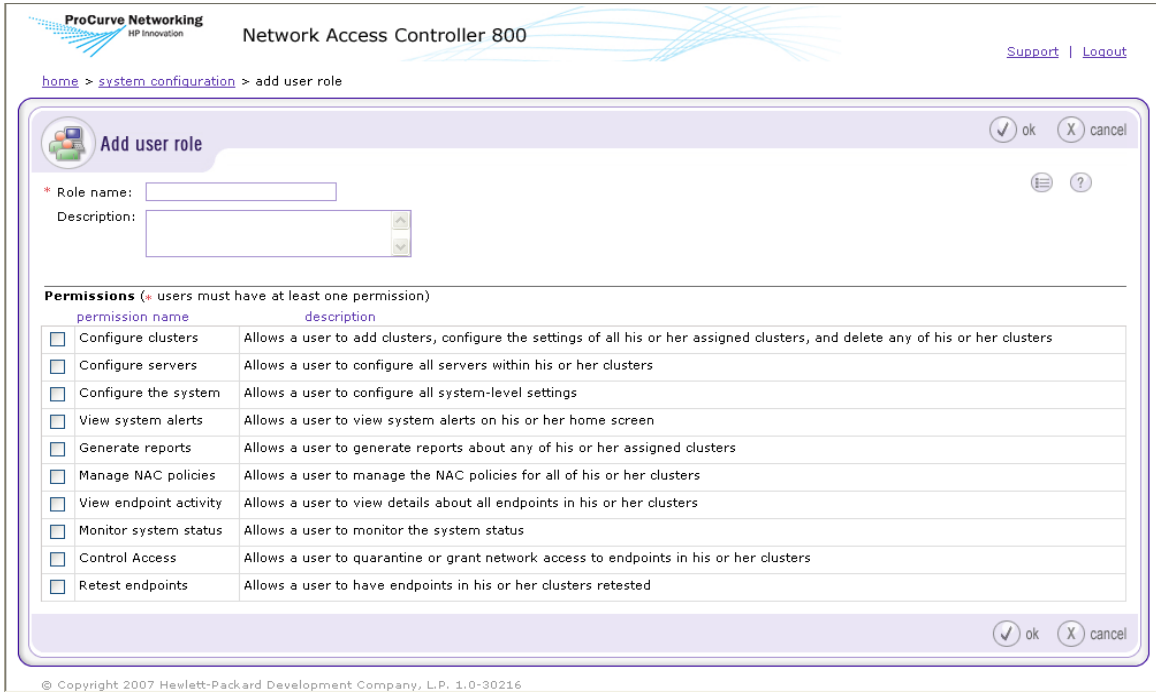

ProCurve Networking
HP Innovation
Network Access Controller 800
Support | Logout
home > system configuration > add user role
Add user role
ok
cancel
* Role name:
Description:
Permissions (* users must have at least one permission)
permission name
description
Configure clusters
Allows a user to add clusters, configure the settings of all his or her assigned clusters, and delete any of his or her clusters
Configure servers
Allows a user to configure all servers within his or her clusters
Configure the system
Allows a user to configure all system-level settings
View system alerts
Allows a user to view system alerts on his or her home screen
Generate reports
Allows a user to generate reports about any of his or her assigned clusters
Manage NAC policies
Allows a user to manage the NAC policies for all of his or her clusters
View endpoint activity
Allows a user to view details about all endpoints in his or her clusters
Monitor system status
Allows a user to monitor the system status
Control Access
Allows a user to quarantine or grant network access to endpoints in his or her clusters
Retest endpoints
Allows a user to have endpoints in his or her clusters retested
ok
cancel
© Copyright 2007 Hewlett-Packard Development Company, L.P. 1.0-30216

Figure 3-16. Add User Role Window

2. Enter a descriptive name in the **Role name** field.
3. Enter a description of the role in the **Description** field.
4. Select the permissions for the user role. For more information about permissions, the following table:

Permission	Description
Configure clusters	Allows you to add clusters, configure the settings of all your assigned clusters, and delete any of your clusters.
Configure servers	Allows you to configure all servers within your clusters
Configure the system	Allows you to configure all system-level settings
View system alerts	Allows you to view system alerts on your home screen
Generate reports	Allows you to generate reports about any of your assigned clusters

Table 3-3.User Role Permissions

Permission	Description
Manage NAC policies	Allows you to manage the NAC policies for all of your clusters
View endpoint activity	Allows you to view details about all endpoints in your clusters
Monitor system status	Allows you to monitor the system status
Control Access	Allows you to quarantine or grant network access to endpoints in your clusters
Retest endpoints	Allows you to have endpoints in your clusters retested

Table 3-3.User Role Permissions (cont.)

Editing User Roles

NOTE: You cannot edit the System Administrator user role.

To edit user roles:

NAC 800 Home window>>System configuration>>User roles

1. Click the role you want to edit. The **user role** window appears:

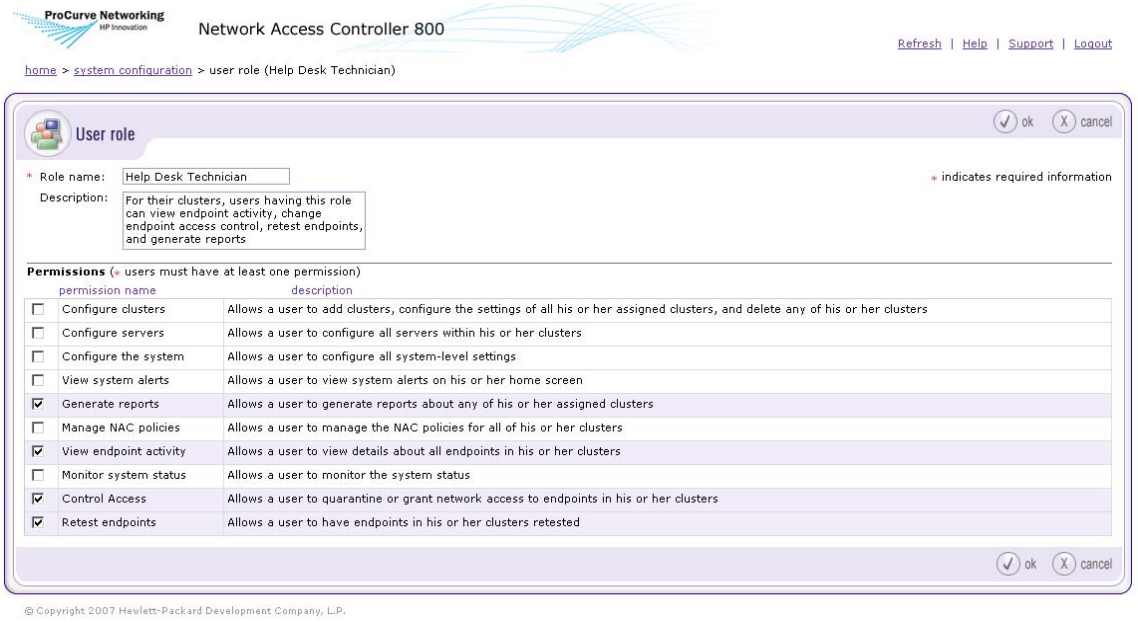

ProCurve Networking
HP Innovation
Network Access Controller 800
Refresh | Help | Support | Logout
home > system configuration > user role (Help Desk Technician)
User role
ok
cancel
* Role name: Help Desk Technician
Description: For their clusters, users having this role can view endpoint activity, change endpoint access control, retest endpoints, and generate reports
* indicates required information
Permissions (* users must have at least one permission)
permission name
description
Configure clusters
Allows a user to add clusters, configure the settings of all his or her assigned clusters, and delete any of his or her clusters
Configure servers
Allows a user to configure all servers within his or her clusters
Configure the system
Allows a user to configure all system-level settings
View system alerts
Allows a user to view system alerts on his or her home screen
Generate reports
Allows a user to generate reports about any of his or her assigned clusters
Manage NAC policies
Allows a user to manage the NAC policies for all of his or her clusters
View endpoint activity
Allows a user to view details about all endpoints in his or her clusters
Monitor system status
Allows a user to monitor the system status
Control Access
Allows a user to quarantine or grant network access to endpoints in his or her clusters
Retest endpoints
Allows a user to have endpoints in his or her clusters retested
ok
cancel
© Copyright 2007 Hewlett-Packard Development Company, L.P.

Figure 3-17. User Role Window

2. Enter the information in the fields you want to change. See "Adding a User Role" on page 3-37 for information on user role settings.
3. Click **ok**.

Deleting User Roles

NOTE: You cannot delete the System Administrator role.

To delete user roles:

NAC 800 Home window>>System configuration>>User roles

1. Click **delete** next to the user role you want to remove. The **Delete user role** confirmation window appears.
2. Click **yes**.

Sorting the User Roles Area

To sort the user roles area:

NAC 800 Home window>>System configuration>>User roles

1. Click **user role name** or **description** column heading. The selected category sorts in ascending or descending order.
2. Click **ok**.

License

The **License** menu option allows you to configure the following:

- View license start and end dates
- View number of days remaining on license, and associated renewal date
- View remaining endpoints and servers available under license

Updating Your License

To update your license:

NAC 800 Home window>>System configuration>>License

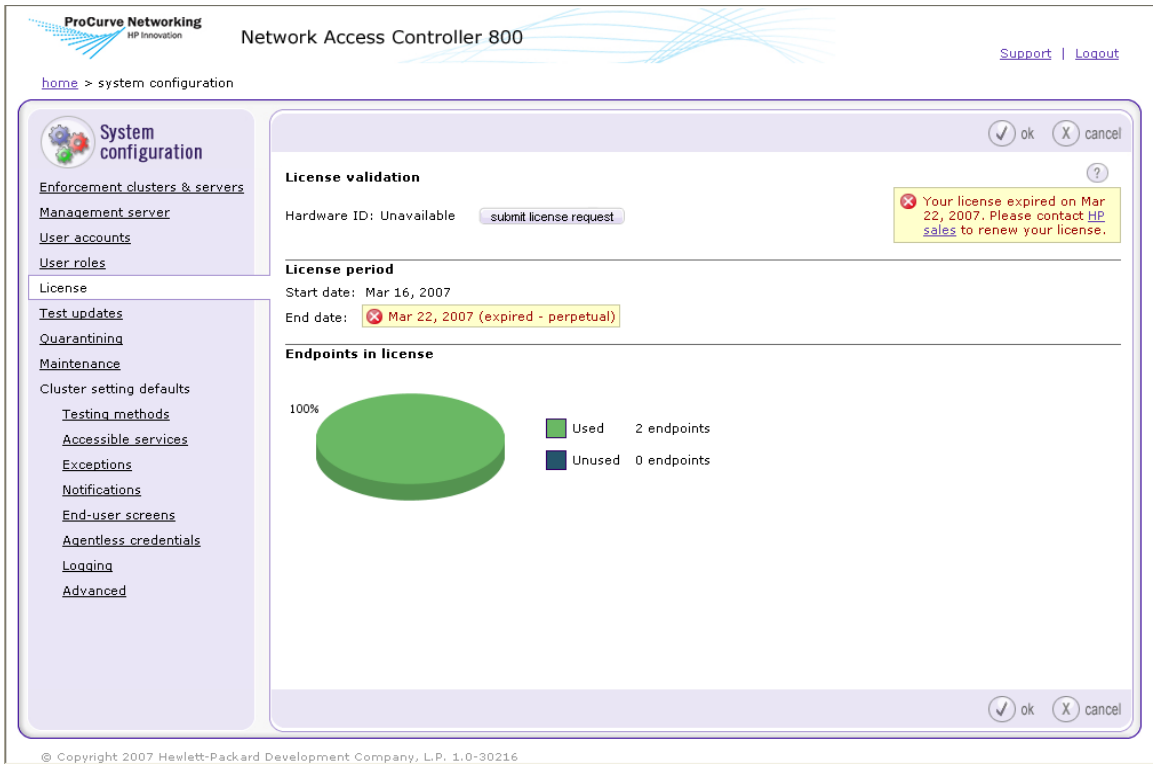


Figure 3-18. System Configuration Window, License

1. Click **submit license request**.
2. Click **ok** on the license validated pop-up window.

Test Updates

The **Test updates** menu option allows you to configure the following:

- View last successful test update date/time
- Check for test updates (forces an immediate check for test updates)
- Set time or times for downloading test updates
- View test update logs

Manually Checking for Test Updates

To manually check for test updates:

NAC 800 Home window>>System configuration>>Test updates

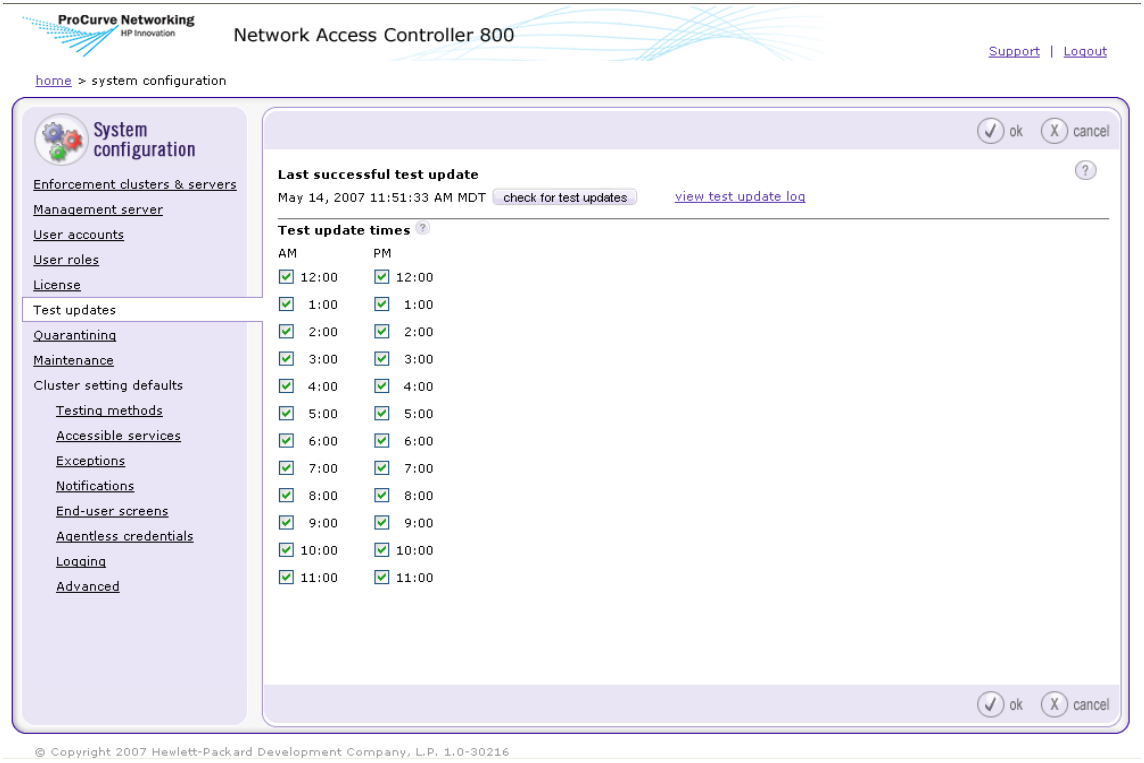


Figure 3-19. System Configuration Window, Test Updates

1. In the **Last successful test update** area, click **check for test updates**.
2. Click **ok**.

NOTE: It is important to check for test updates during the initial configuration of NAC 800.

Selecting Test Update Times

To select test update times:

NAC 800 Home window>>System configuration>>Test updates

1. Using the hour check boxes, select the time periods in which you would like NAC 800 to check for available test updates.

   By default, NAC 800 checks once every hour using the ProCurve Secure Rule Distribution Center. All times listed are dependent upon the clock setting and time zone of the hardware on which NAC 800 is running.

2. Click **ok**.

Viewing Test Update Logs

To view test update logs:

NAC 800 Home window>>System configuration>>Test updates

1. Click the **View test update log** link just to the right of the **Check for test updates** button. The **Test update log** window appears:

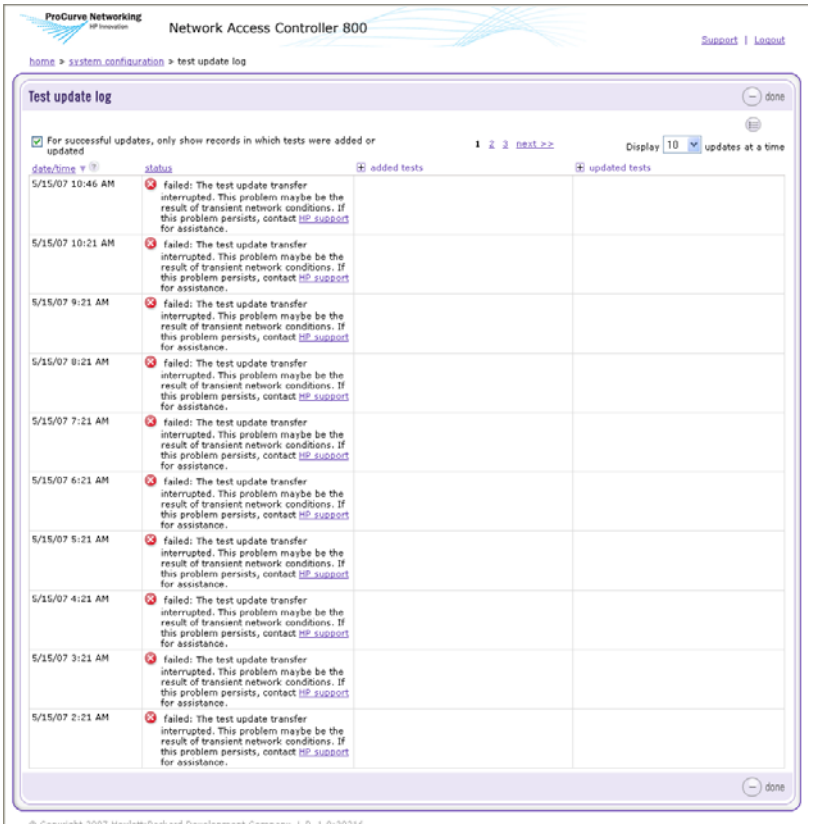

ProCurve Networking
Network Access Controller 800
Support | Logout
home » system configuration » test update log
Test update log
done
For successful updates, only show records in which tests were added or updated
1 2 3 next >>
Display 10 updates at a time
date/time
status
added tests
updated tests
5/15/07 10:46 AM
failed: The test update transfer interrupted. This problem maybe be the result of transient network conditions. If this problem persists, contact HP support for assistance.
5/15/07 10:21 AM
failed: The test update transfer interrupted. This problem maybe be the result of transient network conditions. If this problem persists, contact HP support for assistance.
5/15/07 9:21 AM
failed: The test update transfer interrupted. This problem maybe be the result of transient network conditions. If this problem persists, contact HP support for assistance.
5/15/07 8:21 AM
failed: The test update transfer interrupted. This problem maybe be the result of transient network conditions. If this problem persists, contact HP support for assistance.
5/15/07 7:21 AM
failed: The test update transfer interrupted. This problem maybe be the result of transient network conditions. If this problem persists, contact HP support for assistance.
5/15/07 6:21 AM
failed: The test update transfer interrupted. This problem maybe be the result of transient network conditions. If this problem persists, contact HP support for assistance.
5/15/07 5:21 AM
failed: The test update transfer interrupted. This problem maybe be the result of transient network conditions. If this problem persists, contact HP support for assistance.
5/15/07 4:21 AM
failed: The test update transfer interrupted. This problem maybe be the result of transient network conditions. If this problem persists, contact HP support for assistance.
5/15/07 3:21 AM
failed: The test update transfer interrupted. This problem maybe be the result of transient network conditions. If this problem persists, contact HP support for assistance.
5/15/07 2:21 AM
failed: The test update transfer interrupted. This problem maybe be the result of transient network conditions. If this problem persists, contact HP support for assistance.
done

Figure 3-20. Test Update Log Window

The Test update log window legend is shown in the following figure:

Figure 3-21. Test Update Log Window Legend

Quarantining

The Quarantining menu option allows you to configure the following by cluster:

- Select the quarantine method
- Basic 802.1X settings
- Set up authentication method
- Add, edit, delete 802.1X devices

Selecting the Quarantine Method

To select the quarantine method:

NAC 800 Home window>>System configuration>>Quarantining

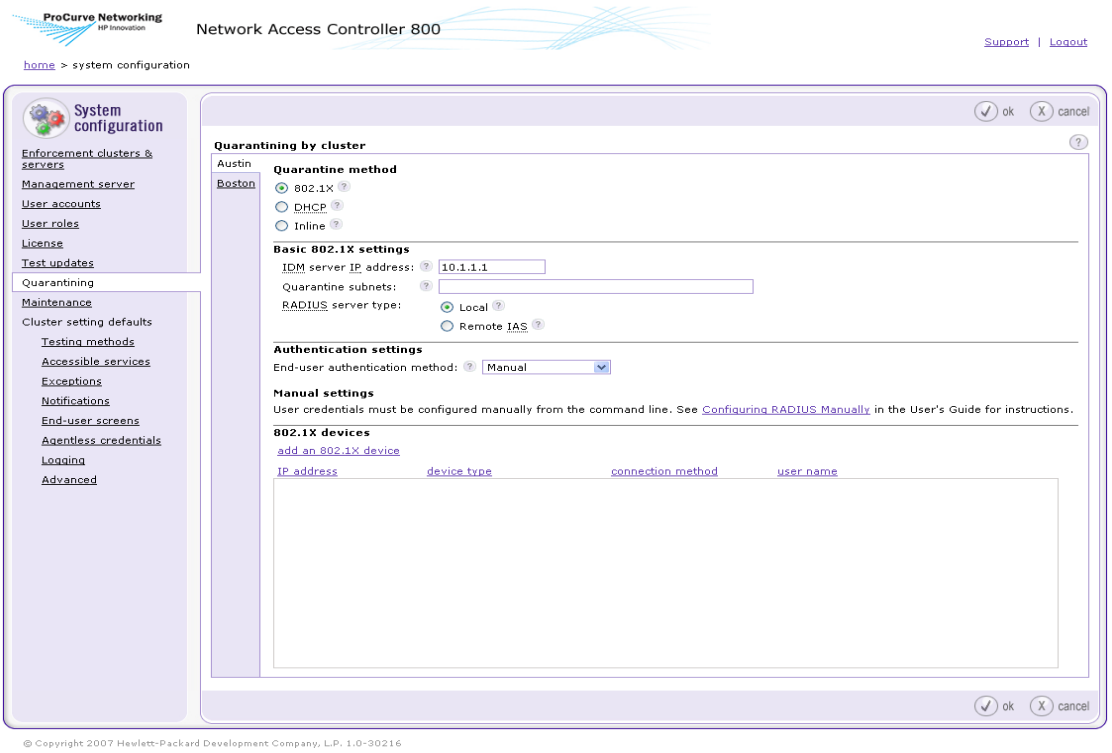


Figure 3-22. System Configuration Window, Quarantining

1. Select a cluster.
2. In the **Quarantine method** area, select one of the following quarantine methods:
   - **802.1X** – When using the 802.1X quarantine method, NAC 800 must sit in a place on the network where it can communicate with your RADIUS server, which communicates with your switch or router, which performs the quarantining.
   - **DHCP** – When configured with a DHCP quarantine area, NAC 800 must sit inline with your DHCP server. All endpoints requesting a DHCP IP address are issued a temporary address on a quarantine subnetwork. Once the endpoint is allowed access, the IP address is renewed, and the main DHCP server assigns an address to the main LAN. With a multiple subnetwork or VLAN network, one quarantine area must be configured for each sub-network.

- **Inline** – When using the inline quarantine method, NAC 800 must be placed on the network where all traffic to be quarantined passes through NAC 800. It must be inline with an endpoint like a VPN.

3. Click **ok**.

Entering Basic 802.1X Settings

To enter basic 802.1X settings:

NAC 800 home window>>System configuration>>Quarantining>>802.1X quarantine method radio button

1. Enter an IP address in the Identity Driven Manager (**IDM**) **server IP address** text field.
2. Enter one or more non-quarantined subnets, separated by commas in the **Quarantine subnets** text field. All subnets should be entered using CIDR addresses.
3. Select a **RADIUS server type** by selecting one of the following radio buttons:
   - **Local** – Enables a local RADIUS server on the Enforcement server which can be configured to perform authentication itself or proxy to another server.
   - **Remote IAS** – Disables the local RADIUS server so that an IAS server configured with the NAC IAS plug-in to point to an Enforcement server can be used instead. When possible, a local RADIUS server that proxies to the IAS server should be the preferred configuration.
4. Click **ok**.

Selecting the RADIUS Authentication method

To select the RADIUS authentication method:

NAC 800 home window>>System configuration>>Quarantining>>802.1X quarantine method radio button

1. Select the **Local** radio button in the **Basic 802.1X settings** area.
2. Select an **End-user authentication method**:
   - **Manual** – RADIUS server authentication settings are configured manually from the command line. See “Enabling NAC 800 for 802.1X” on page 11-43 for configuration information.

- **Windows domain** – Authentication requests are handled by a Windows domain through NTLM protocol. The Enforcement server must be able to join to the domain for this to work. See “Configuring Windows Domain Settings” on page 3-52 for more information.
- **OpenLDAP** – User credentials are queried from an OpenLDAP directory service. See “Configuring OpenLDAP Settings” on page 3-54 for more information.
- **Novell eDirectory** – User credentials are queried from a Novell eDirectory directory service. See “Configuring Novell eDirectory Settings” on page 3-57 for more information.
- **Proxy** – Authentication requests are proxied to a remote RADIUS server configured to allow the Enforcement server as a client NAS.

3. Click **ok**.

Configuring Windows Domain Settings

To configure Windows domain settings:

NAC 800 home window>>System configuration>>Quarantining>>802.1X Quarantine method radio button>>Local radio button

1. Select **Windows domain** from the **End-user authentication method** drop-down list.

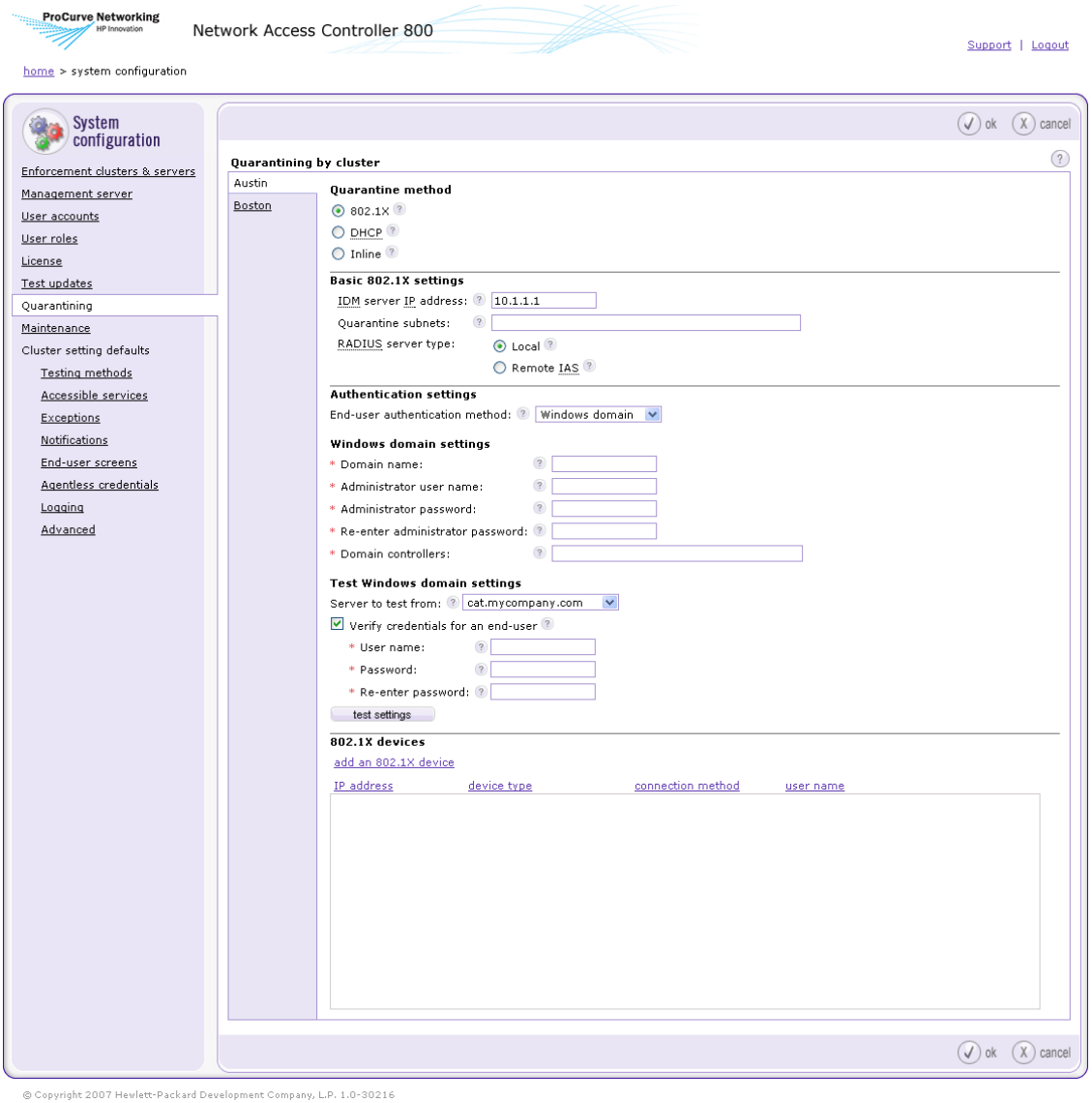


Figure 3-23. System Configuration, Windows Domain Window

2. Enter the Fully Qualified Domain Name (FQDN) of the domain to be joined in the **Domain name** text field.

3. Enter the user name of an account with sufficient administrative rights to join an Enforcement server to the domain in the **Administrator user name** text field.
4. Enter the password of the account entered into the **Administrator user name** field in the **Administrator password** text field.
5. Enter the list of domain controllers, separated by commas, for this domain in the **Domain controllers** text field.
6. To test the Windows domain settings:
   a. Select one of the following from the **Server to test from** drop-down list in the **Test Windows domain settings area**:
      – The Enforcement server in this cluster to test from, or
      – The management server

NOTE: If you have a single-server installation, the Server to test from drop-down list is not available.

   b. To verify a specific set of user credentials in addition to the Windows domain settings, select the **Verify credentials for an end-user** check box, and specify the following:
      i. Enter the user name of the end-user in the **User name** text box.
      ii. Enter the password of the end-user in the **Password** text box.
      iii. Re-enter the password of the end-user in the **Re-enter password** text box.
   c. Click **test settings**.
7. Click **ok**.

Configuring OpenLDAP Settings

To configure OpenLDAP settings:

NAC 800 home window>>System configuration>>Quarantining>>802.1X Quarantine method radio button>>Local radio button

1. Select **OpenLDAP** from the **End-user authentication method** drop-down list.

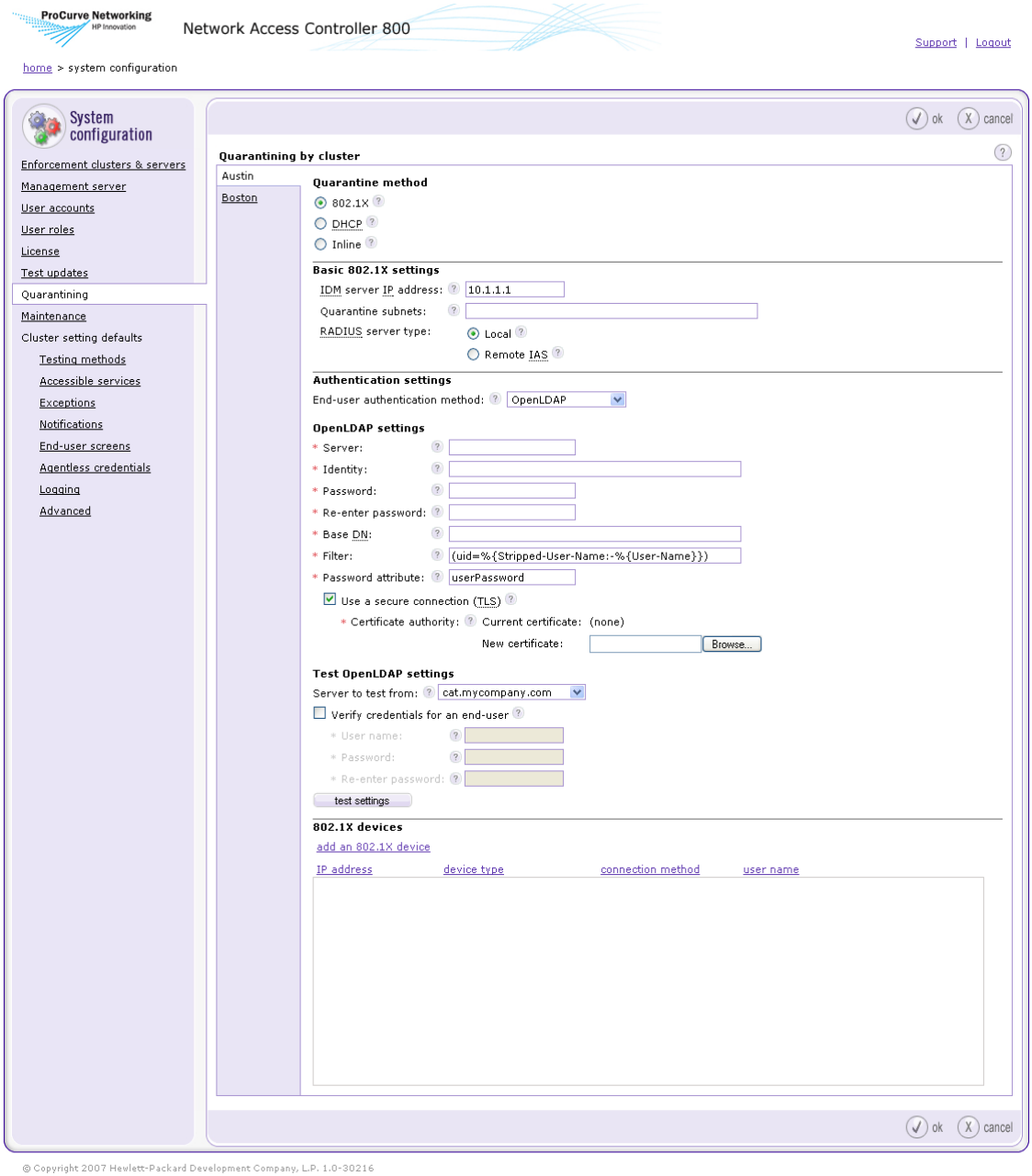


Figure 3-24. System Configuration Window, OpenLDAP

2. Enter the LDAP server hostname or IP address and optional port number in the **Server** text field. For example: `10.0.1.2:636`
3. Enter the DN under which LDAP searches should be done in the **Identity** text field. For example: `cn=admin,o=My Org,c=UA`
4. Enter the password that authenticates the DN entered into the **Identity** text field in the **Password** text field.
5. Type the same password you entered into the **Password** field in the **Re-enter password** field.
6. Enter the base DN of LDAP searches in the **Base DN** text field. For example: `o=My Org,c=UA`
7. Enter the LDAP search filter used to locate user objects from name supplied by endpoint in the **Filter** text field. For example: `(uid=%u)`
8. Enter the LDAP attribute which contains end-user passwords in the **Password attribute** text field. This is initially set to `userPassword` to use the universal password of the eDirectory user.
9. To use a secure Transport Layer Security (TLS) connection with the LDAP server that is verified with a certificate authority:
   a. Select the **Use a secure connection (TLS)** check box.
   b. Enter a PEM-encoded file name that contains the CA certificate used to sign the LDAP server's TLS certificate in the **New certificate** text field. Click **Browse** to search for file names. The current certificate selected is shown by **Current certificate**.
10. To test the OpenLDAP settings:
    a. Select one of the following from the **Server to test from** drop-down list in the **Test Windows domain settings area**:
       – The Enforcement server in this cluster to test from, or
       – The management server
    b. To verify a specific set of user credentials in addition to the OpenLDAP settings, select the **Verify credentials for an end-user** check box, and specify the following:
       i. Enter the user name of the end-user in the **User name** text box.
       ii. Enter the password of the end-user in the **Password** text box.
       iii. Re-enter the password of the end-user in the **Re-enter password** text box.
    c. Click **test settings**.
11. Click **ok**.

Configuring Novell eDirectory Settings

To configuring Novell eDirectory settings:

NAC 800 home window>>System configuration>>Quarantining>>802.1x Quarantine method radio button>>Local radio button

1. Select **Novell eDirectory** from the End-user authentication type drop-down list.

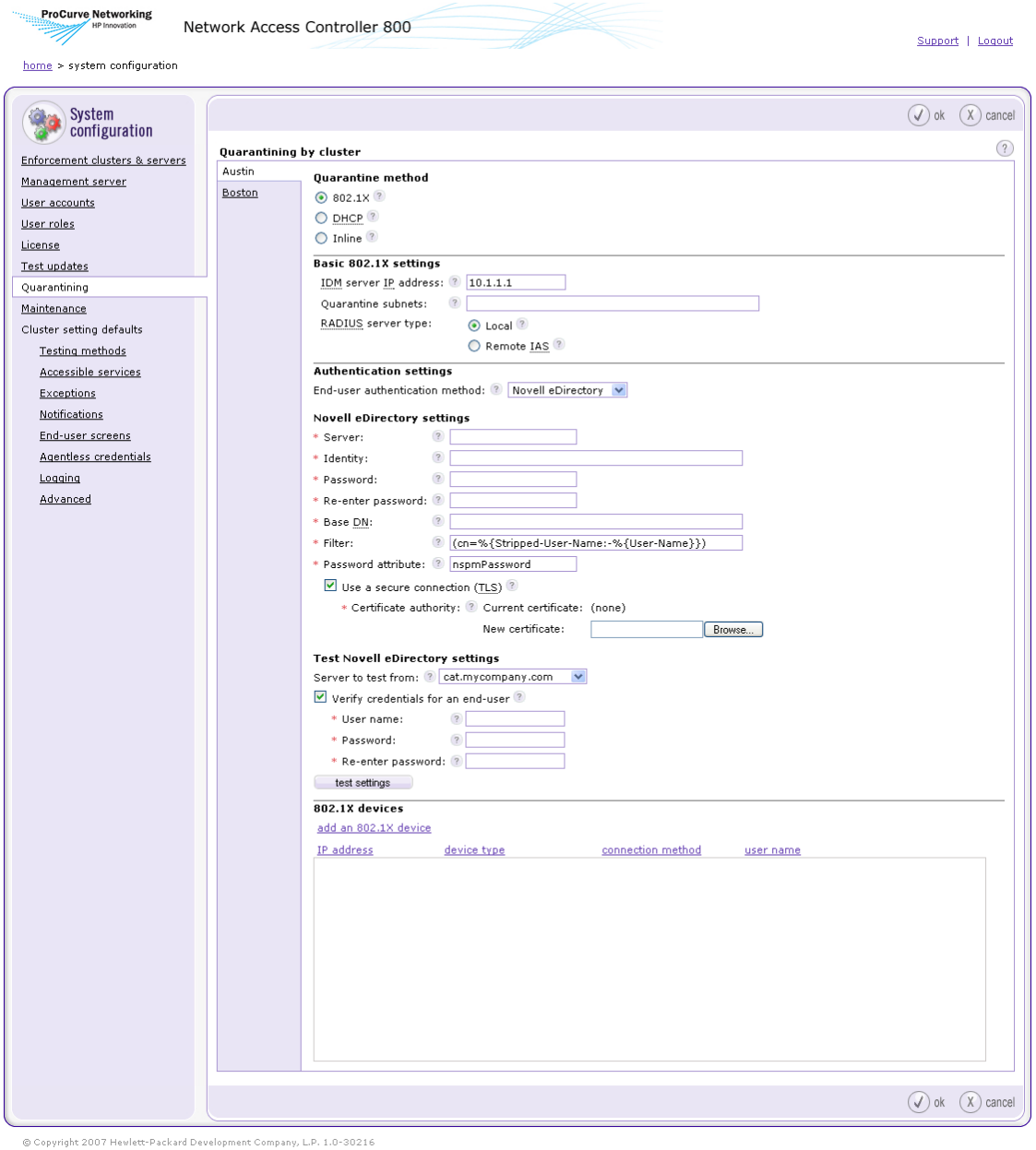


Figure 3-25. System Configuration Window, RADIUS, Novel eDirectory

2. Enter the LDAP server hostname or IP address and optional port number in the **Server** text field. For example: `10.0.1.2:636`
3. Enter the Distinguished Name (DN) under which LDAP searches should be done in the **Identity** text field. For example: `cn=admin,o=My Org,c=UA`
4. Enter the password that authenticates the DN entered into the **Identity** text field in the **Password** text field.
5. Type the same password you entered into the **Password** field in the **Re-enter password** field.
6. Enter the base DN in LDAP Data Interchange Format (LDIF) under which user queries should be performed in the **Base DN** text field. For example: `o=My Org,c=UA`
7. Enter the LDAP search filter used to locate user objects from name supplied by endpoint in the **Filter** text field. For example: `(uid=%u)`
8. Enter the LDAP attribute which contains end-user passwords in the **Password attribute** text field. This is initially set to `nspmPassword` to use the universal password of the eDirectory user.
9. To use a secure Transport Layer Security (TLS) connection with the LDAP server that is verified with a certificate authority:
   a. Select the **Use a secure connection (TLS)** check box.
   b. Enter a PEM-encoded file name that contains the CA certificate used to sign the LDAP server's TLS certificate in the **New certificate** text field. Click **Browse** to search for file names. The current certificate selected is shown by **Current certificate**.
10. To test the Novell eDirectory settings:
    a. For multiple-server installations: Select one of the following from the **Server to test from** drop-down list in the **Test Windows domain settings area**:
       – The enforcement server in this cluster to test from, or
       – The management server
    b. To verify a specific set of user credentials in addition to the Novell eDirectory settings, select the **Verify credentials for an end-user** check box, and specify the following:
       i. Enter the user name of the end-user in the **User name** text box.
       ii. Enter the password of the end-user in the **Password** text box.
       iii. Re-enter the password of the end-user in the **Re-enter password** text box.
    c. Click **test settings**.

11. Click **ok**.

Adding 802.1X Devices

To add an 802.1X device:

NAC 800 home window>>System configuration>>Quarantining>>802.1X Quarantine method radio button>>Add an 802.1X device

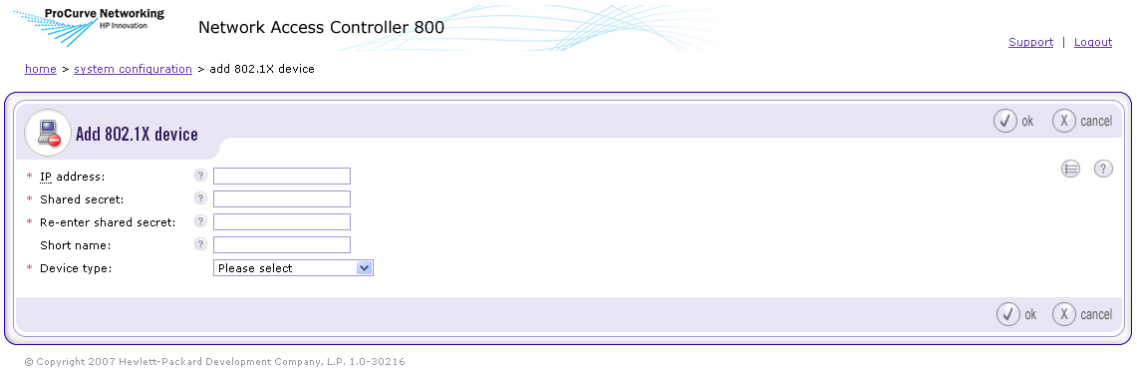


Figure 3-26. Add 802.1X Device Window

1. Enter the IP address of the 802.1X device in the **IP address** text field.
2. Enter a shared secret in the **Shared secret** text field. The shared secret is used to encrypt and sign packets between the device and RADIUS server.
3. Re-enter the shared secret in the **Re-enter shared secret** text field.
4. Enter an alias for this device that appears in log files in the **Short name** text field.
5. Select an 802.1X device from the **Device type** drop-down list.
6. Enter the configuration settings for the specific device:
   - **Cisco IOS** – See “Cisco IOS” on page 3-62.
   - **Cisco CatOS** – See “Cisco CatOS” on page 3-63.
   - **Enterasys** – See “Enterasys” on page 3-65.
   - **Extreme ExtremeWare** – See “Extreme ExtremeWare” on page 3-67.
   - **Extreme XOS** – See “Extreme XOS” on page 3-69.
   - **Foundry** – See “Foundry” on page 3-71.

- **HP ProCurve switch** – See “HP ProCurve Switch” on page 3-73.
- **HP ProCurve WESM** – See “HP ProCurve WESM” on page 3-76.
- **HP ProCurve 420/530 AP** – See “HP ProCurve 420 AP or HP ProCurve 530 AP” on page 3-79.
- **Nortel** – See “Nortel” on page 3-81.
- **Other** – See “Other” on page 3-83.

7. Click **ok**.

Testing the Connection to a Device

To test the connection to an 802.1X device:

NAC 800 home window>>System configuration>>Quarantining>>802.1X Quarantine method radio button

NOTE: You must have already added devices for them to appear in the 802.1X devices area. You can also test the device as you add it.

1. In the **802.1X devices** area, click **edit** next to the device you want to test. The **802.1X device** window appears. The Test connection to this device area is near the bottom of the window:

Figure 3-27. Add 802.1X Device, Test Connection Area

2. Optional: If you want to include the re-authentication command as part of the test, select the Re-authenticate an endpoint during test check box and:
   a. Enter the port of the endpoint being tested in the **Port** text field.
   b. Enter the MAC address of the endpoint being tested in the **MAC address** text field.

NOTE: You must enter the port, the MAC address, or both, depending on the re-authentication OID.

3. Click **test connection to device**.

Cisco IOS

To add a Cisco IOS device:

NAC 800 home window>>System configuration>>Quarantining>>802.1X Quarantine method radio button>>Add an 802.1X device

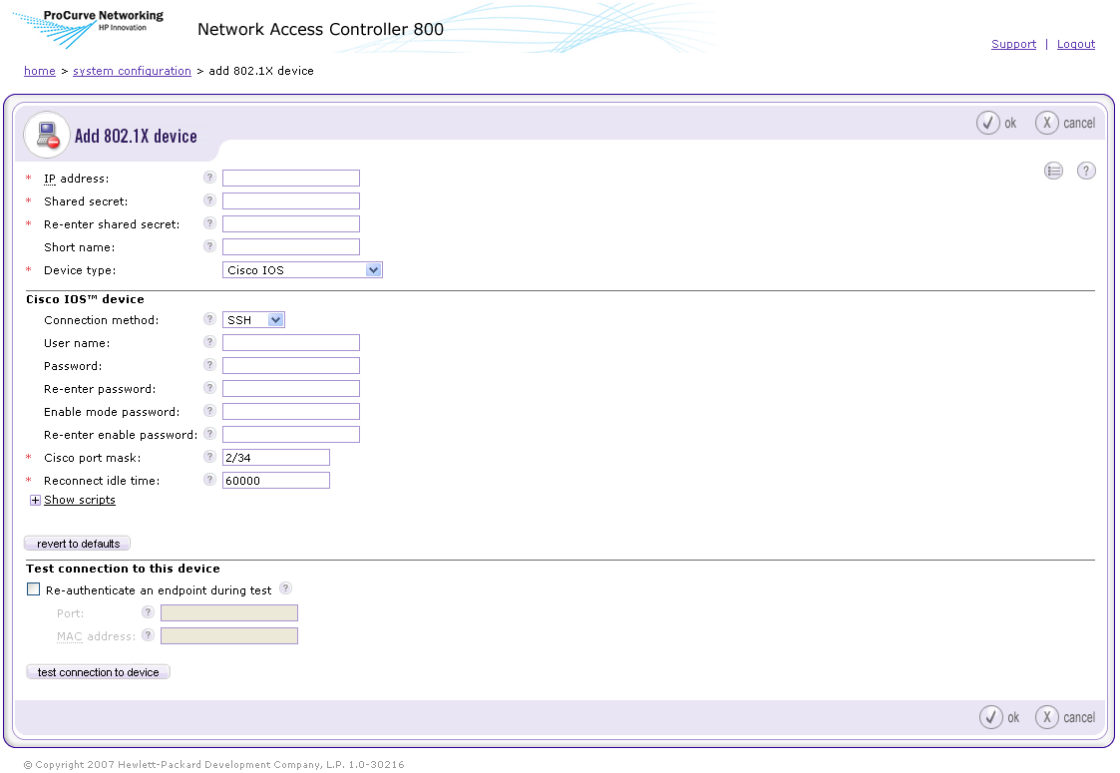


Figure 3-28. Add Cisco IOS Device Window

1. Enter the IP address of the Cisco IOS device in the **IP address** text field.
2. Enter a shared secret in the **Shared secret** text field. The shared secret is used to encrypt and sign packets between the device and RADIUS server.
3. Re-enter the shared secret in the **Re-enter shared secret** text field.

4. Enter an alias for this device that appears in log files in the **Short name** text field.
5. Select **Cisco IOS** from the **Device type** drop-down list.
6. Select telnet or SSH from the **Connection method** drop-down list.
7. Enter the **User name** with which to log into the device's console.
8. Enter the **Password** with which to log into the device's console.
9. Re-enter the console password.
10. Enter the **Cisco port mask** in the text field. This specifies which characters within the endpoint identifier returned by the Cisco device contain the bank and port information of the endpoint. All offsets start at 0, so a mask of 2/34 indicates character 3 for the bank and characters 4 and 5 for the port. If the Cisco device were to return 50210 for an endpoint, a port mask of 2/34 would indicate that the endpoint is on bank 2 and port 10 (2/10), where 210 are the third, fourth and fifth bytes in the identifier.
11. Enter the **Reconnect idle time**. This is the amount of time in milliseconds that a telnet/SSH console can remain idle or unused before it is reset.
12. Select the **Show scripts** plus symbol to show the following scripts:
    - **Initialization script** – The expect script used to log into the console and enter enable mode.
    - **Re-authentication script** – The expect script used to perform endpoint re-authentication.
    - **Exit script** – The expect script used to exit the console.
13. Click **ok**.

TIP: Click revert to defaults to restore the default settings.

Cisco CatOS

To add a Cisco CatOS device:

NAC 800 home window>>System configuration>>Quarantining>>802.1X Quarantine method radio button>>Add an 802.1X device

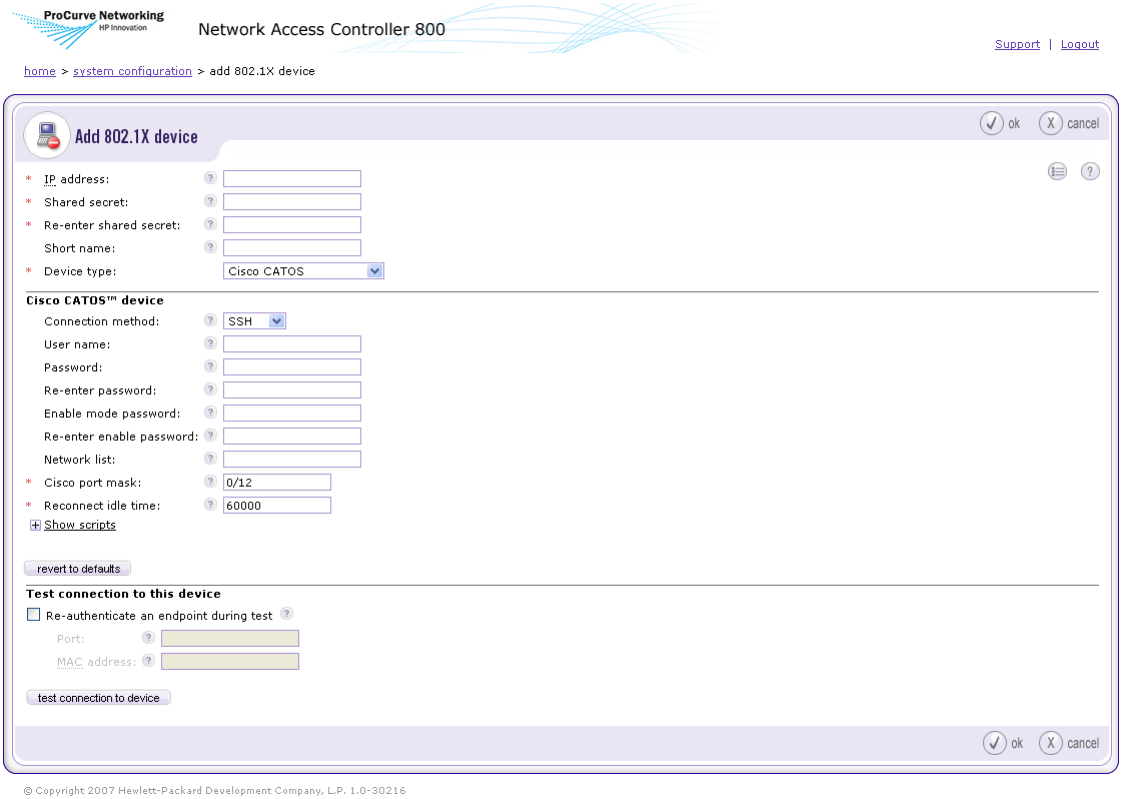


Figure 3-29. Add Cisco CatOS Device Window

1. Enter the IP address of the Cisco CatOS device in the **IP address** text field.
2. Enter a shared secret in the **Shared secret** text field. The shared secret is used to encrypt and sign packets between the device and RADIUS server.
3. Re-enter the shared secret in the **Re-enter shared secret** text field.
4. Enter an alias for this device that appears in log files in the **Short name** text field.
5. Select **Cisco CatOS** from the **Device type** drop-down list.
6. Select telnet or SSH from the **Connection method** drop-down list.
7. Enter the **User name** with which to log into the device's console.
8. Enter the **Password** with which to log into the device's console.

9. Re-enter the console password.
10. Enter the password with which to enter enable mode.
11. Re-enter the enable mode password.
12. Enter the networks (using CIDR notation) that this device is in direct control over in the **Network list** text field. This is only necessary if the device does not send its IP address with its supplicant request.
13. Enter the **Cisco port mask** in the text field. This specifies which characters within the endpoint identifier returned by the Cisco device contain the bank and port information of the endpoint. All offsets start at 0, so a mask of 2/34 indicates character 3 for the bank and characters 4 and 5 for the port. If the Cisco device were to return 50210 for an endpoint, a port mask of 2/34 would indicate that the endpoint is on bank 2 and port 10 (2/10), where 210 are the third, fourth and fifth bytes in the identifier.
14. Enter the **Reconnect idle time**. This is the amount of time in milliseconds that a telnet/SSH console can remain idle or unused before it is reset.
15. Select the **Show scripts** plus symbol to show the following scripts:
    - **Initialization script** – The expect script used to log into the console and enter enable mode.
    - **Re-authentication script** – The expect script used to perform endpoint re-authentication.
    - **Exit script** – The expect script used to exit the console.
16. Click **ok**.

TIP: Click revert to defaults to restore the default settings.

Enterasys

To add an Enterasys device:

NAC 800 home window>>System configuration>>Quarantining>>802.1X Quarantine method radio button>>Add an 802.1X device

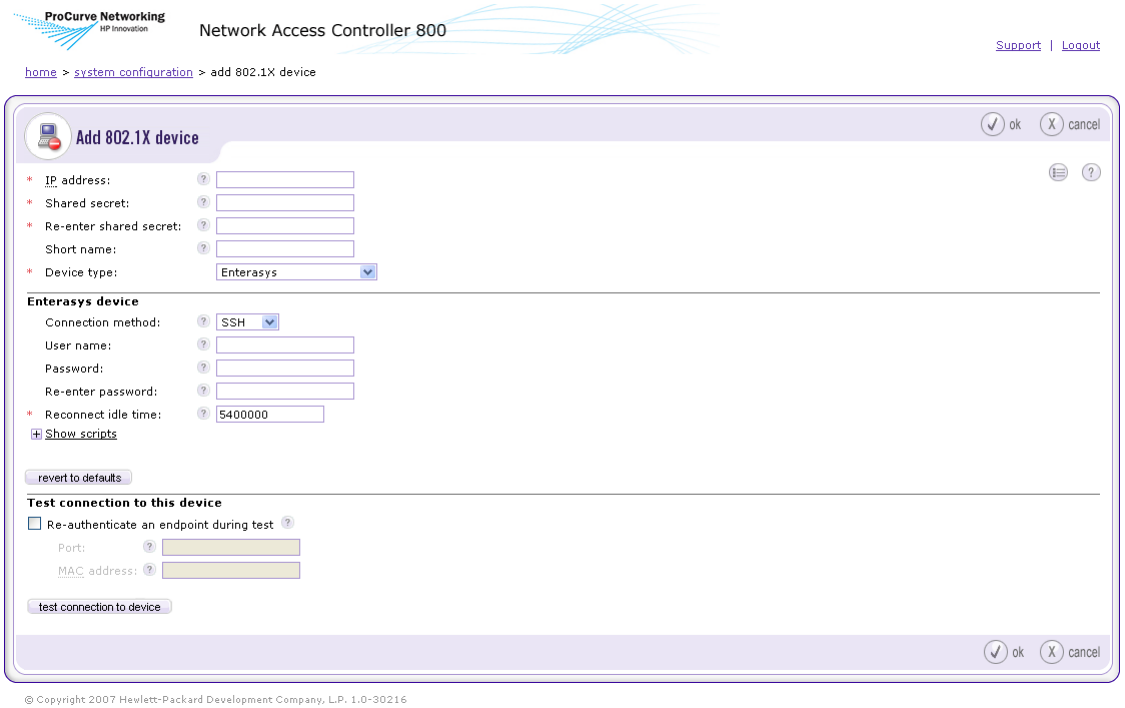


Figure 3-30. Add Enterasys Device Window

1. Enter the IP address of the Enterasys device in the **IP address** text field.
2. Enter a shared secret in the **Shared secret** text field. The shared secret is used to encrypt and sign packets between the device and RADIUS server.
3. Re-enter the shared secret in the **Re-enter shared secret** text field.
4. Enter an alias for this device that appears in log files in the **Short name** text field.
5. Select **Enterasys** from the **Device type** drop-down list.
6. Select telnet or SSH from the **Connection method** drop-down list.
7. Enter the **User name** with which to log into the device's console.
8. Enter the **Password** with which to log into the device's console.
9. Re-enter the console password.

10. Enter the **Reconnect idle time**. This is the amount of time in milliseconds that a telnet/SSH console can remain idle or unused before it is reset.
11. Select the **Show scripts** plus symbol to show the following scripts:
    - **Initialization script** – The expect script used to log into the console and enter enable mode.
    - **Re-authentication script** – The expect script used to perform endpoint re-authentication.
    - **Exit script** – The expect script used to exit the console.
12. Click **ok**.

TIP: Click revert to defaults to restore the default settings.

Extreme ExtremeWare

To add an ExtremeWare device:

NAC 800 home window>>System configuration>>Quarantining>>802.1X Quarantine method radio button>>Add an 802.1X device

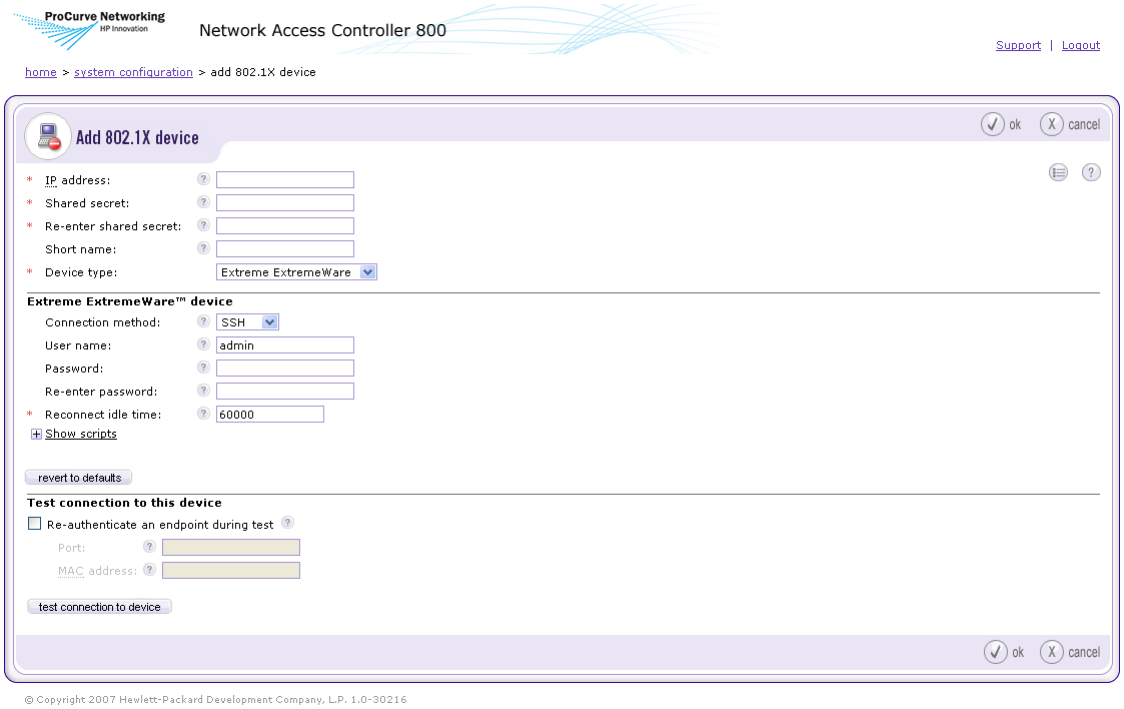


Figure 3-31. Add ExtremeWare Device Window

1. Enter the IP address of the ExtremeWare device in the **IP address** text field.
2. Enter a shared secret in the **Shared secret** text field. The shared secret is used to encrypt and sign packets between the device and RADIUS server.
3. Re-enter the shared secret in the **Re-enter shared secret** text field.
4. Enter an alias for this device that appears in log files in the **Short name** text field.
5. Select **Extreme ExtremeWare** from the **Device type** drop-down list.
6. Select telnet or SSH from the **Connection method** drop-down list.
7. Enter the **User name** with which to log into the device's console.
8. Enter the **Password** with which to log into the device's console.
9. Re-enter the console password.
10. Enter the **Reconnect idle time**. This is the amount of time in milliseconds that a telnet/SSH console can remain idle or unused before it is reset.

11. Select the **Show scripts** plus symbol to show the following scripts:
    - **Initialization script** – The expect script used to log into the console and enter enable mode.
    - **Re-authentication script** – The expect script used to perform endpoint re-authentication.
    - **Exit script** – The expect script used to exit the console.
12. Click **ok**.

TIP: Click revert to defaults to restore the default settings.

Extreme XOS

To add an Extreme XOS device:

NAC 800 home window>>System configuration>>Quarantining>>802.1X Quarantine method radio button>>Add an 802.1X device

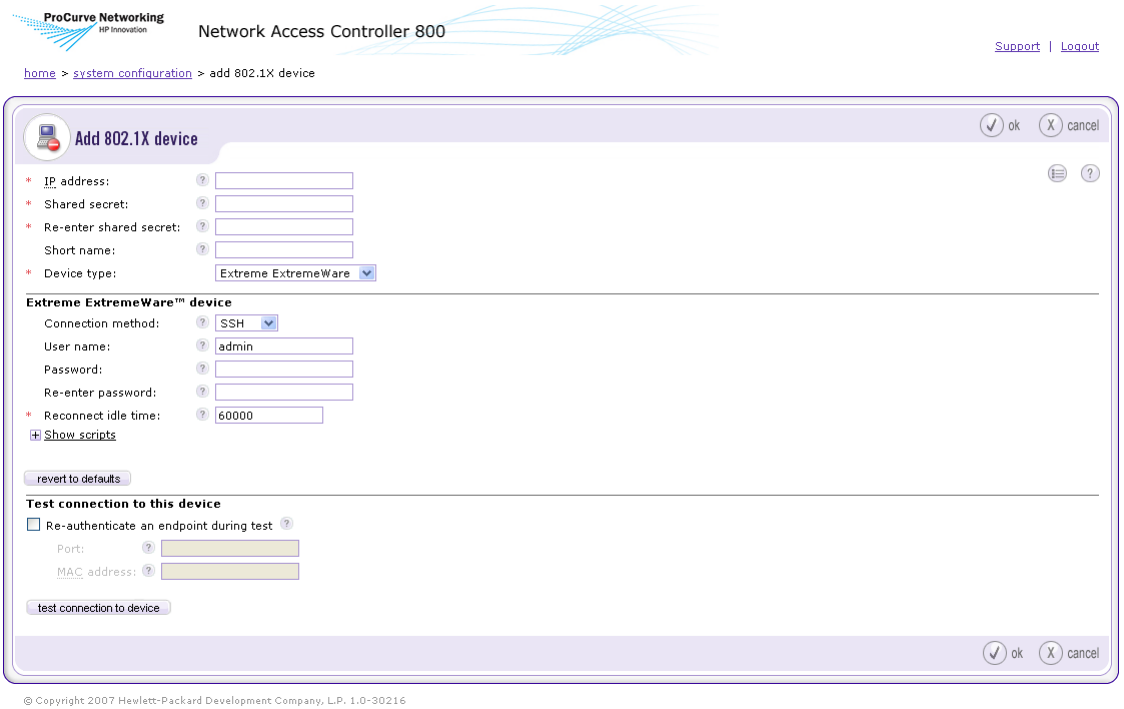


Figure 3-32. Add Extreme XOS Device Window

1. Enter the IP address of the Extreme XOS device in the **IP address** text field.
2. Enter a shared secret in the **Shared secret** text field. The shared secret is used to encrypt and sign packets between the device and RADIUS server.
3. Re-enter the shared secret in the **Re-enter shared secret** text field.
4. Enter an alias for this device that appears in log files in the **Short name** text field.
5. Select **Extreme XOS** from the **Device type** drop-down list.
6. Select telnet or SSH from the **Connection method** drop-down list.
7. Enter the **User name** with which to log into the device's console.
8. Enter the **Password** with which to log into the device's console.
9. Enter the **Reconnect idle time**. This is the amount of time in milliseconds that a telnet/SSH console can remain idle or unused before it is reset.

10. Select the **Show scripts** plus symbol to show the following scripts:
    - **Initialization script** – The expect script used to log into the console and enter enable mode.
    - **Re-authentication script** – The expect script used to perform endpoint re-authentication.
    - **Exit script** – The expect script used to exit the console.
11. Click **ok**.

TIP: Click revert to defaults to restore the default settings.

Foundry

To add a Foundry device:

NAC 800 home window>>System configuration>>Quarantining>>802.1X Quarantine method radio button>>Add an 802.1X device

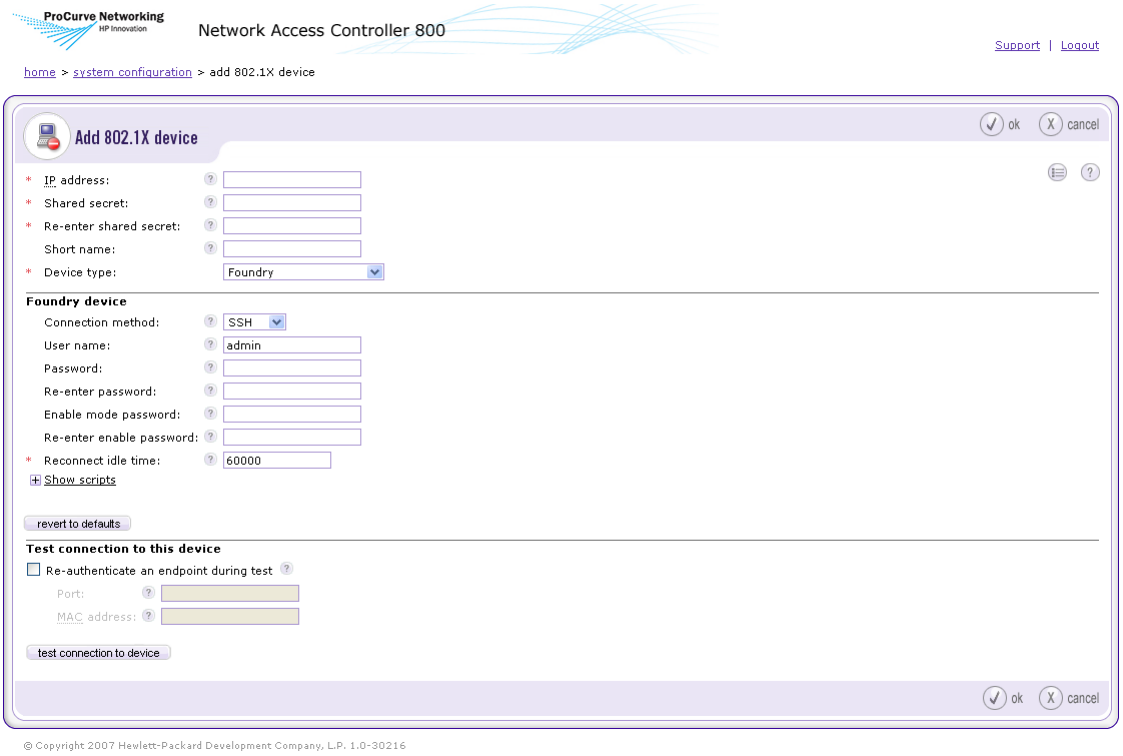


Figure 3-33. Add Foundry Device Window

1. Enter the IP address of the Foundry device in the **IP address** text field.
2. Enter a shared secret in the **Shared secret** text field. The shared secret is used to encrypt and sign packets between the device and RADIUS server.
3. Re-enter the shared secret in the **Re-enter shared secret** text field.
4. Enter an alias for this device that appears in log files in the **Short name** text field.
5. Select **Foundry** from the **Device type** drop-down list.
6. Select telnet or SSH from the **Connection method** drop-down list.
7. Enter the **User name** with which to log into the device's console.
8. Enter the **Password** with which to log into the device's console.
9. Re-enter the console password.

10. Enter the password with which to enter enable mode.
11. Re-enter the enable mode password.
12. Enter the **Reconnect idle time**. This is the amount of time in milliseconds that a telnet/SSH console can remain idle or unused before it is reset.
13. Select the **Show scripts** plus symbol to show the following scripts:
    - **Initialization script** – The expect script used to log into the console and enter enable mode.
    - **Re-authentication script** – The expect script used to perform endpoint re-authentication.
    - **Exit script** – The expect script used to exit the console.
14. Click **ok**.

TIP: Click revert to defaults to restore the default settings.

HP ProCurve Switch

To add an HP ProCurve switch:

NAC 800 home window>>System configuration>>Quarantining>>802.1X Quarantine method radio button>>Add an 802.1X device

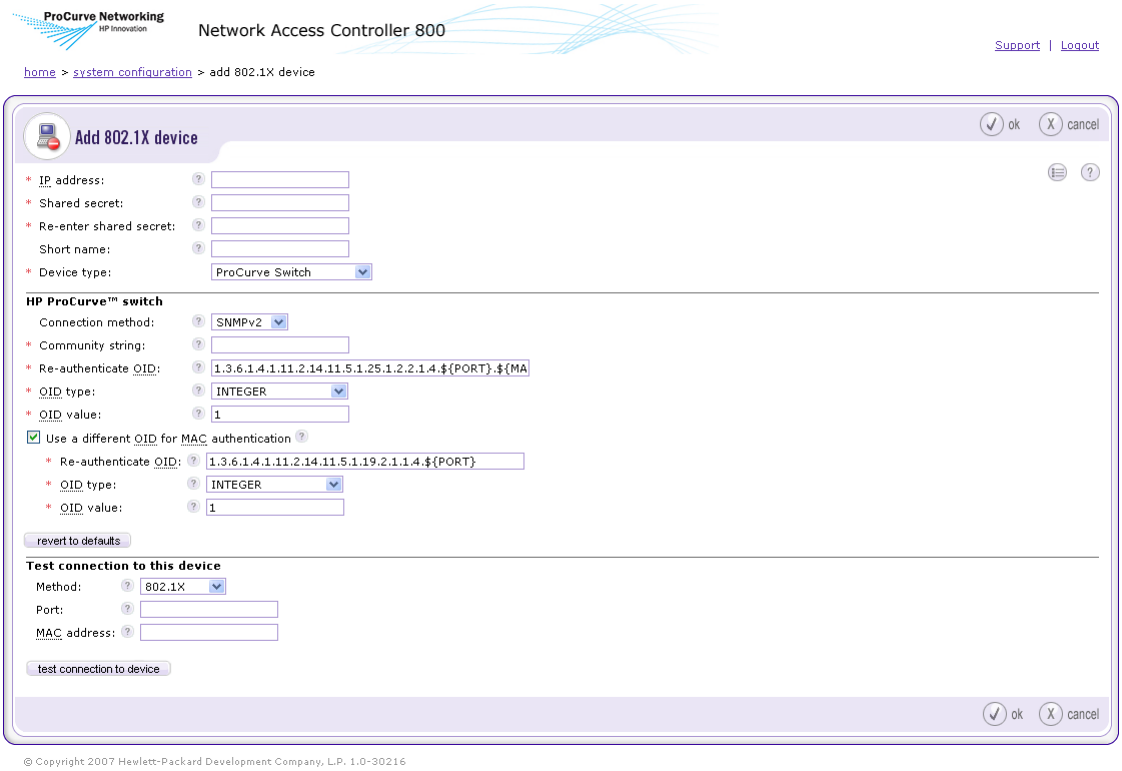


Figure 3-34. Add HP ProCurve Device Window

1. Enter the IP address of the HP ProCurve device in the **IP address** text field.
2. Enter a shared secret in the **Shared secret** text field. The shared secret is used to encrypt and sign packets between the device and RADIUS server.
3. Re-enter the shared secret in the **Re-enter shared secret** text field.
4. Enter an alias for this device that appears in log files in the **Short name** text field.
5. Select **ProCurve Switch** from the **Device type** drop-down list.
6. Select whether to connect to this device using telnet, SSH, or SNMPv2 in the **Connection method** drop-down list.
7. SSH settings:
   a. Enter the **User name** used to log into this device's console.
   b. Enter the **Password** used to log into this device's console.

c. To help confirm accuracy, type the same password you entered into the **Password** field in the **Re-enter Password** field.

d. Enter the **Enable mode user name** that is used to enter enable mode on this device.

e. Enter the **Password** used to enter enable mode on this device.

f. To help confirm accuracy, type the same password you entered into the **Enable** password field in the **Re-enter Password** field.

g. Enter the amount of time, in milliseconds, before an idle open SSH session is reset. The default is 60000 (60 seconds) in the **Reconnect idle time** field.

8. Telnet settings:

a. Enter the **User name** used to log into this device's console.

b. Enter the **Password** used to log into this device's console.

c. To help confirm accuracy, type the same password you entered into the **Password** field in the **Re-enter Password** field.

d. Enter the **Enable mode user name** that is used to enter enable mode on this device.

e. Enter the **Password** used to enter enable mode on this device.

f. To help confirm accuracy, type the same password you entered into the **Enable** password field in the **Re-enter Password** field.

g. Enter the amount of time, in milliseconds, before an idle open telnet session is reset. The default is 60000 (60 seconds) in the **Reconnect idle time** field.

9. SNMPv2 settings:

a. Enter the **Community string** used to authorize writes to SNMP objects.

b. Enter the OID used to re-authenticate an endpoint in the **Re-authenticate OID** text field. The strings "${Port}" and "${MAC}" will be substituted for the port and MAC address of the endpoint to be re-authenticated.

c. Select the type of the re-authentication OID from the **OID type** drop-down list:
   - INTEGER
   - unsigned INTEGER
   - TIMETICKS
   - IPADDRESS
   - OBJID
   - STRING
   - HEX STRING
   - DECIMAL STRING
   - BITS

- NULLOBJ

d. Enter the OID re-authentication value used to re-authenticate an endpoint in the **OID value** text field.

e. Select the **Use a different OID for MAC authentication** check box to re-authenticate using a different OID when the supplicant request is for a MAC authenticated device.

i. Enter the **Re-authenticate OID** used to re-authenticate an endpoint. The strings "${PORT}" and "${MAC_DOTTED_DECIMAL}" are substituted for the port and MAC address of the endpoint to be re-authenticated.

ii. Select the type of the re-authentication OID from the **OID type** drop-down list:

- INTEGER
- unsigned INTEGER
- TIMETICKS
- IPADDRESS
- OBJID
- STRING
- HEX STRING
- DECIMAL STRING
- BITS
- NULLOBJ

iii. Enter the OID re-authentication value used to re-authenticate an endpoint in the **OID value** text field.

TIP: Click revert to defaults to restore the default settings.

HP ProCurve WESM

To add an HP ProCurve WESM device:

NAC 800 home window>>System configuration>>Quarantining>>802.1X Quarantine method radio button>>Add an 802.1X device

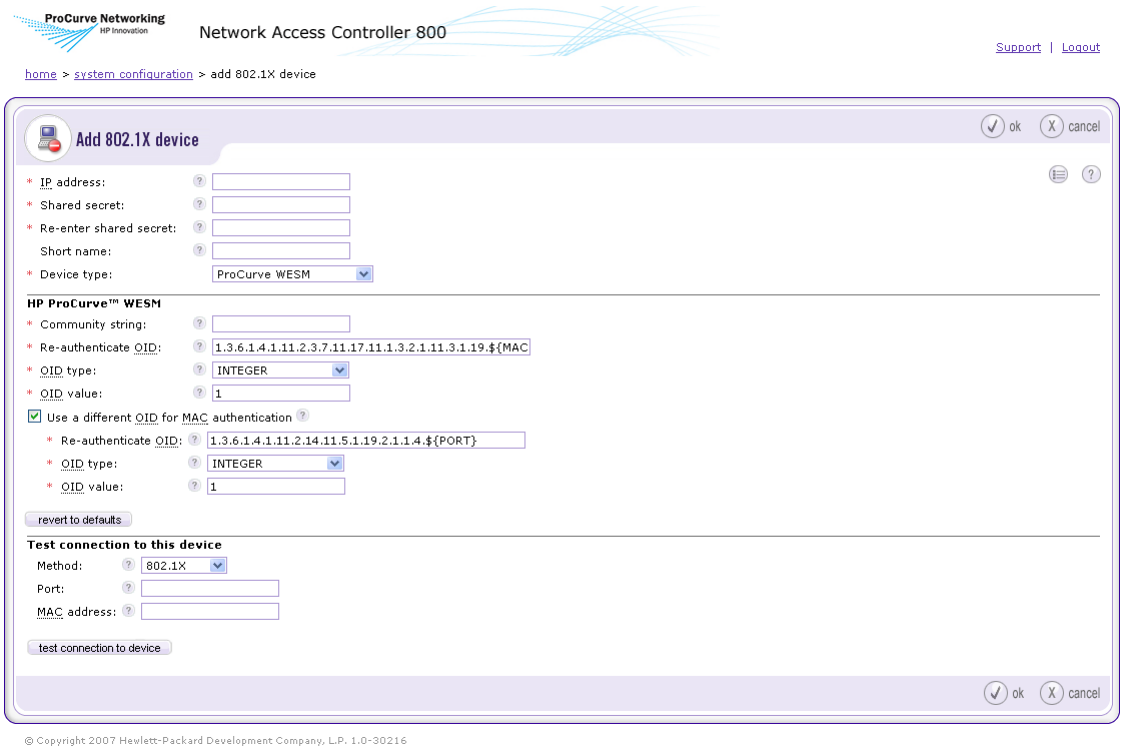


Figure 3-35. Add HP ProCurve WESM Device Window

1. Enter the IP address of the HP ProCurve WESM device in the **IP address** text field.
2. Enter a shared secret in the **Shared secret** text field. The shared secret is used to encrypt and sign packets between the device and RADIUS server.
3. Re-enter the shared secret in the **Re-enter shared secret** text field.
4. Enter an alias for this device that appears in log files in the **Short name** text field.
5. Select **ProCurve WESM** from the **Device type** drop-down list.
6. Enter the **Community string** used to authorize writes to SNMP objects.

7. Enter the OID used to re-authenticate an endpoint in the **Re-authenticate OID** text field. The strings "${Port}" and "${MAC_DOTTED_DECIMAL}" will be substituted for the port and MAC address of the endpoint to be re-authenticated.
8. Select the type of the re-authentication OID from the **OID type** drop-down list:
   - INTEGER
   - unsigned INTEGER
   - TIMETICKS
   - IPADDRESS
   - OBJID
   - STRING
   - HEX STRING
   - DECIMAL STRING
   - BITS
   - NULLOBJ
9. Enter the OID re-authentication value used to re-authenticate an endpoint in the **OID value** text field.
10. Select the **Use a different OID for MAC authentication** check box to re-authenticate using a different OID when the supplicant request is for a MAC authenticated device.
    a. Enter the **Re-authenticate OID** used to re-authenticate an endpoint. The strings "${Port}" and "${MAC_DOTTED_DECIMAL}" are substituted for the port and MAC address of the endpoint to be re-authenticated.
    b. Select the type of the re-authentication OID from the **OID type** drop-down list:
       – INTEGER
       – unsigned INTEGER
       – TIMETICKS
       – IPADDRESS
       – OBJID
       – STRING
       – HEX STRING
       – DECIMAL STRING
       – BITS
       – NULLOBJ
    c. Enter the OID re-authentication value used to re-authenticate an endpoint in the **OID value** text field.

TIP: Click revert to defaults to restore the default settings.

HP ProCurve 420 AP or HP ProCurve 530 AP

To add an HP ProCurve 420 AP or HP ProCurve 530 AP device:

NAC 800 home window>>System configuration>>Quarantining>>802.1X Quarantine method radio button>>Add an 802.1X device

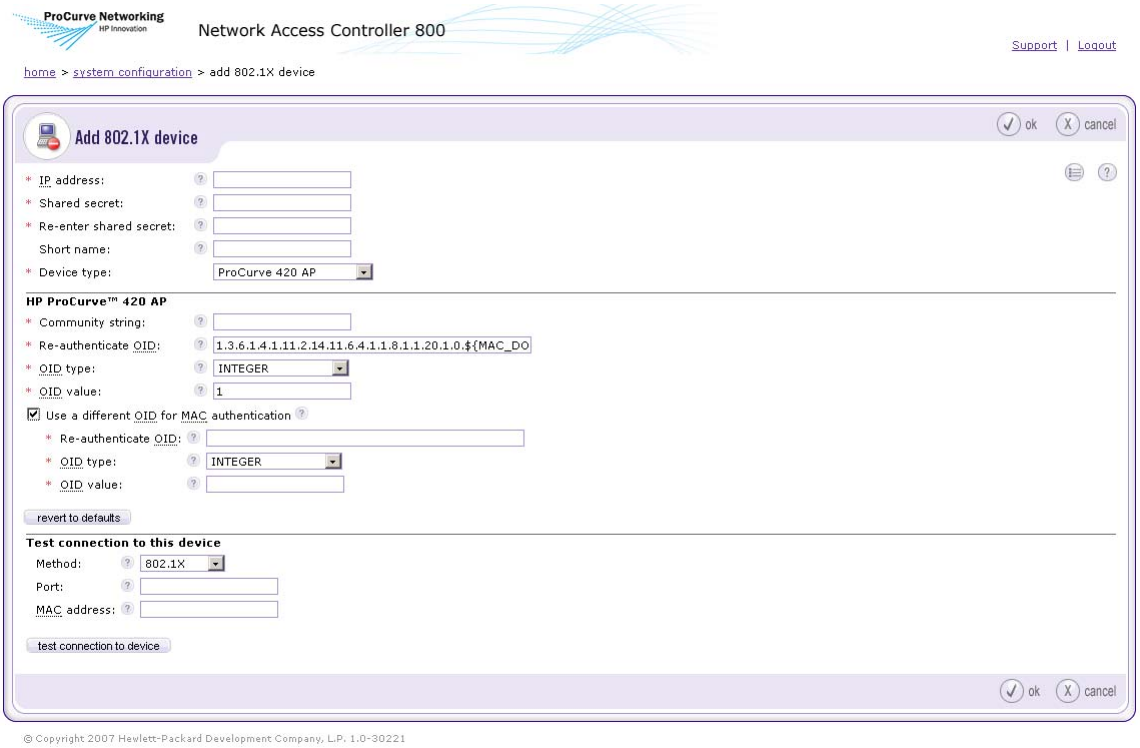


Figure 3-36. Add HP ProCurve 420/530 AP Device Window

1. Enter the IP address of the HP ProCurve AP or HP ProCurve 530 AP device in the **IP address** text field.
2. Enter a shared secret in the **Shared secret** text field. The shared secret is used to encrypt and sign packets between the device and RADIUS server.

3. Re-enter the shared secret in the **Re-enter shared secret** text field.
4. Enter an alias for this device that appears in log files in the **Short name** text field.
5. Select **ProCurve 420 AP or ProCurve 530 AP** from the **Device type** drop-down list.
6. Enter the **Community string** used to authorize writes to SNMP objects.
7. Enter the OID used to re-authenticate an endpoint in the **Re-authenticate OID** text field. The strings "${Port}" and "${MAC_DOTTED_DECIMAL}" will be substituted for the port and MAC address of the endpoint to be re-authenticated.
8. Select the type of the re-authentication OID from the **OID type** drop-down list:
   - INTEGER
   - unsigned INTEGER
   - TIMETICKS
   - IPADDRESS
   - OBJID
   - STRING
   - HEX STRING
   - DECIMAL STRING
   - BITS
   - NULLOBJ
9. Enter the OID re-authentication value used to re-authenticate an endpoint in the **OID value** text field.
10. Select the **Use a different OID for MAC authentication** check box to re-authenticate using a different OID when the supplicant request is for a MAC authenticated device.
    a. Enter the **Re-authenticate OID** used to re-authenticate an endpoint. The strings "${Port}" and "${MAC_DOTTED_DECIMAL}" are substituted for the port and MAC address of the endpoint to be re-authenticated.
    b. Select the type of the re-authentication OID from the **OID type** drop-down list:
       – INTEGER
       – unsigned INTEGER
       – TIMETICKS
       – IPADDRESS
       – OBJID
       – STRING

- HEX STRING
- DECIMAL STRING
- BITS
- NULLOBJ

c. Enter the OID re-authentication value used to re-authenticate an endpoint in the **OID value** text field.

TIP: Click revert to defaults to restore the default settings.

Nortel

To add a Nortel device:

NAC 800 home window>>System configuration>>Quarantining>>802.1X Quarantine method radio button>>Add an 802.1X device

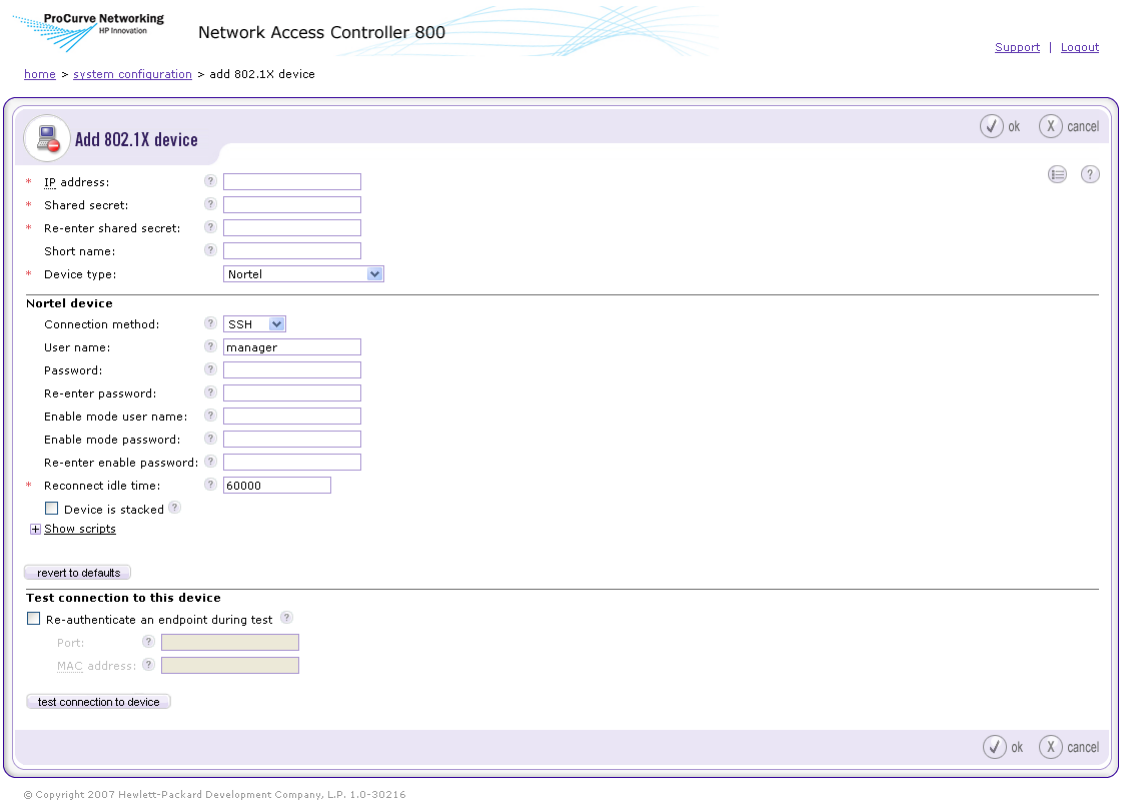


Figure 3-37. Add Nortel Device Window

1. Enter the IP address of the Nortel device in the **IP address** text field.
2. Enter a shared secret in the **Shared secret** text field. The shared secret is used to encrypt and sign packets between the device and RADIUS server.
3. Re-enter the shared secret in the **Re-enter shared secret** text field.
4. Enter an alias for this device that appears in log files in the **Short name** text field.
5. Select **Nortel** from the **Device type** drop-down list.
6. Select telnet or SSH from the **Connection method** drop-down list.
7. Enter the **User name** with which to log into the device's console.
8. Enter the **Password** with which to log into the device's console.

9. Re-enter the console password.
10. Enter the **Enable mode user name**.
11. Enter the password with which to enter enable mode.
12. Re-enter the enable mode password.
13. Enter the **Reconnect idle time**. This is the amount of time in milliseconds that a telnet/SSH console can remain idle or unused before it is reset.
14. Select the **Device is stacked** check box if the device is in a stacked configuration.
15. Select the **Show scripts** plus symbol to show the following scripts:
    - **Initialization script** – The expect script used to log into the console and enter enable mode.
    - **Re-authentication script** – The expect script used to perform endpoint re-authentication.
    - **Exit script** – The expect script used to exit the console.
16. Click **ok**.

TIP: Click revert to defaults to restore the default settings.

Other

To add a non-listed 802.1X device:

NAC 800 home window>>System configuration>>Quarantining>>802.1X Quarantine method radio button>>Add an 802.1X device

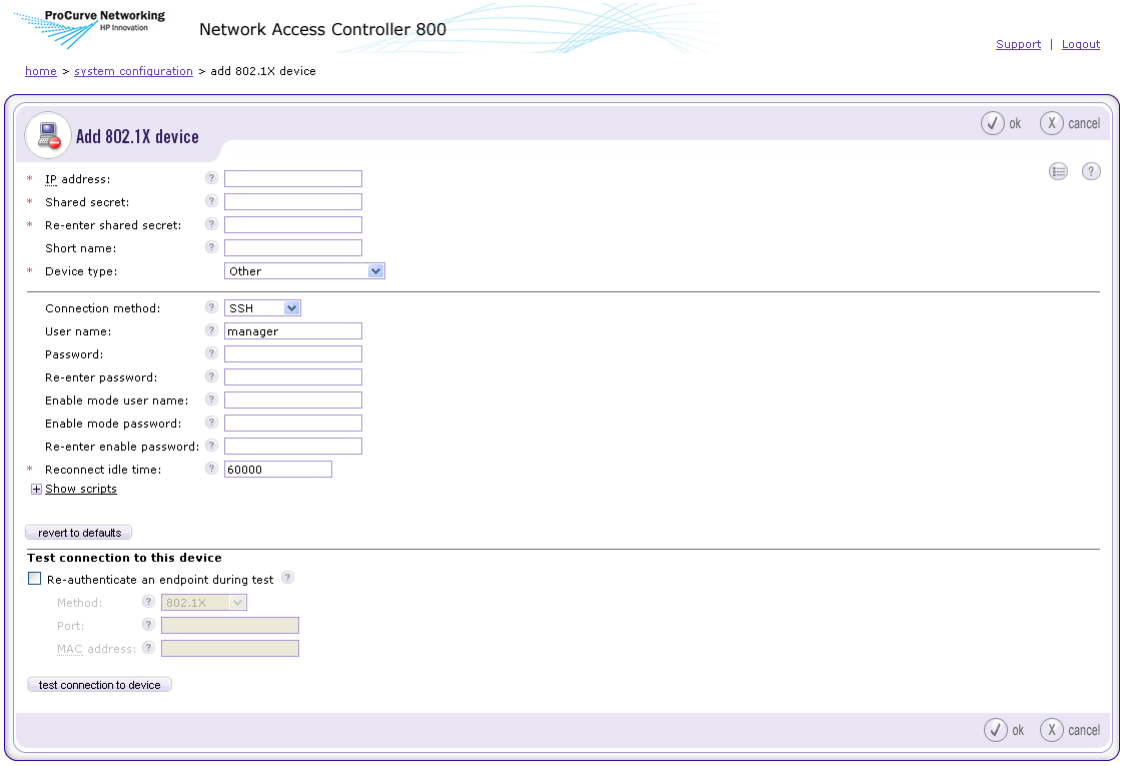


Figure 3-38. Add Other Device Window

1. Enter the IP address of the new device in the **IP address** text field.
2. Enter a shared secret in the **Shared secret** text field. The shared secret is used to encrypt and sign packets between the device and RADIUS server.
3. Re-enter the shared secret in the **Re-enter shared secret** text field.
4. Enter an alias for this device that appears in log files in the **Short name** text field.
5. Select **Other** from the **Device type** drop-down list.
6. Enter the **User name** with which to log into the device's console.
7. Enter the **Password** with which to log into the device's console.
8. Re-enter the console password.

9. Enter the **Reconnect idle time**. This is the amount of time in milliseconds that a telnet/SSH console can remain idle or unused before it is reset.
10. Select the **Show scripts** plus symbol to show the following scripts:

NOTE: You must enter the script contents yourself for the 802.1X device you are adding.

- **Initialization script** – The expect script used to log into the console and enter enable mode.
- **Re-authentication script** – The expect script used to perform endpoint re-authentication.
- **Exit script** – The expect script used to exit the console.

11. Click **ok**.

TIP: Click revert to defaults to restore the default settings.

Setting DHCP Enforcement

NOTE: See "Configuring Windows Update Service for XP SP2" on page 10-5 for information on using Windows Update Service for devices in quarantine.

To set DHCP enforcement:

NAC 800 Home window>>System configuration>>Quarantining>>DHCP quarantine method radio button

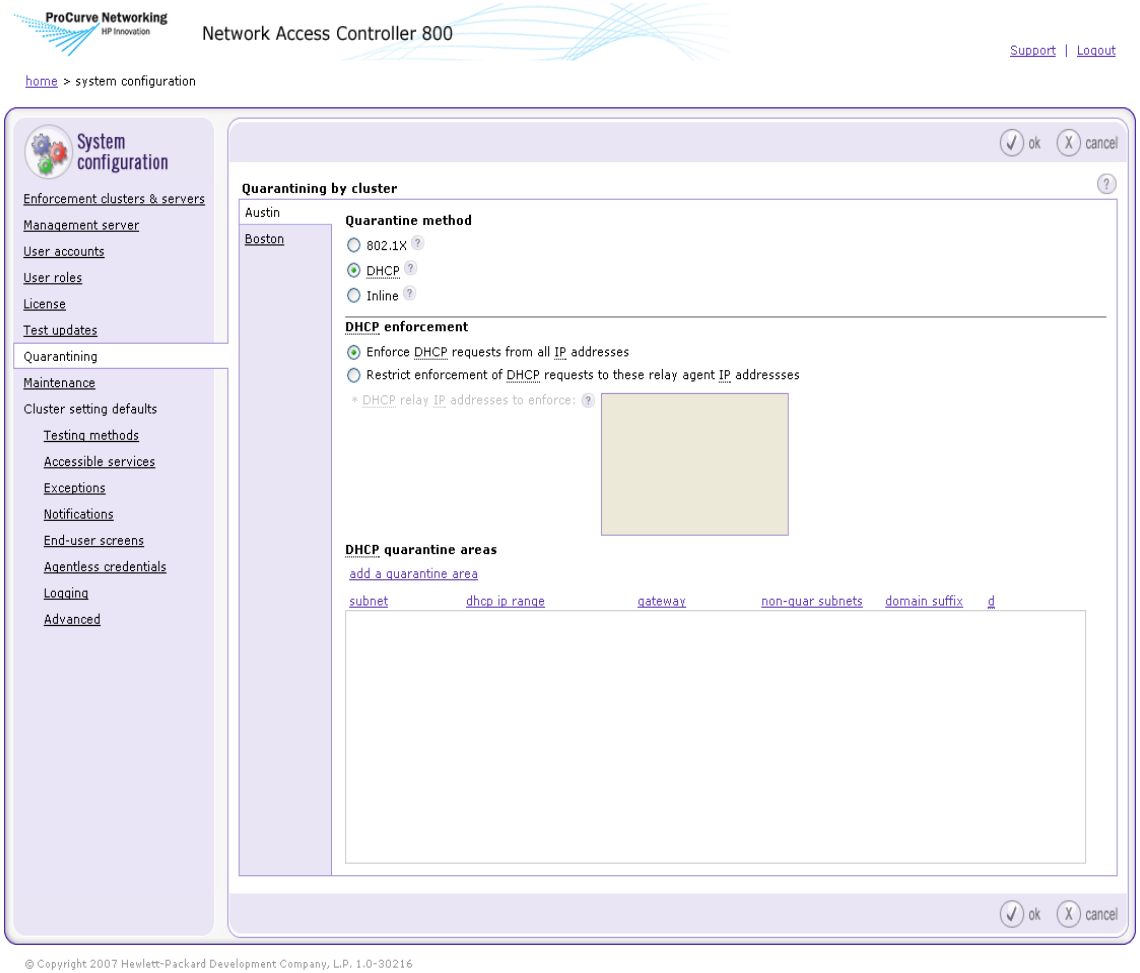


Figure 3-39. DHCP Enforcement Window

1. Select one of the following radio buttons:
   - **Enforce DHCP requests from all IP addresses** – Allows DHCP requests from all IP addresses.
   - **Restrict enforcement of DHCP requests to these relay agent IP addresses** – Specify individual DHCP relay agent IP addresses, separated by carriage returns. in the text box.

     These addresses must be a subset of either the quarantined or non-

quarantined subnets. This limits the enforcement scope to DHCP requests relayed via these IP addresses, allowing you to restrict enforcement to only those DHCP requests which are forwarded via particular routers or layer-3 switches. If set, DHCP traffic coming from a source IP not listed will be passed without intervention.

NOTE:

Construction of the DHCP relay packet's source IP address is vendor-dependent. Some implementations (for example, Extreme) use the IP address of the interface closest to the DHCP server as the source IP for DHCP forwarding, which means the resultant packet may not have a source IP that corresponds to those used on the endpoint's physical subnet. Check your switch vendor's implementation to be sure you are entering correct IP information.

2. Click **ok**.

Adding a DHCP Quarantine Area

To add a quarantine area:

NAC 800 Home window>>System configuration>>Quarantining>>DHCP quarantine method radio button>>add a quarantine area

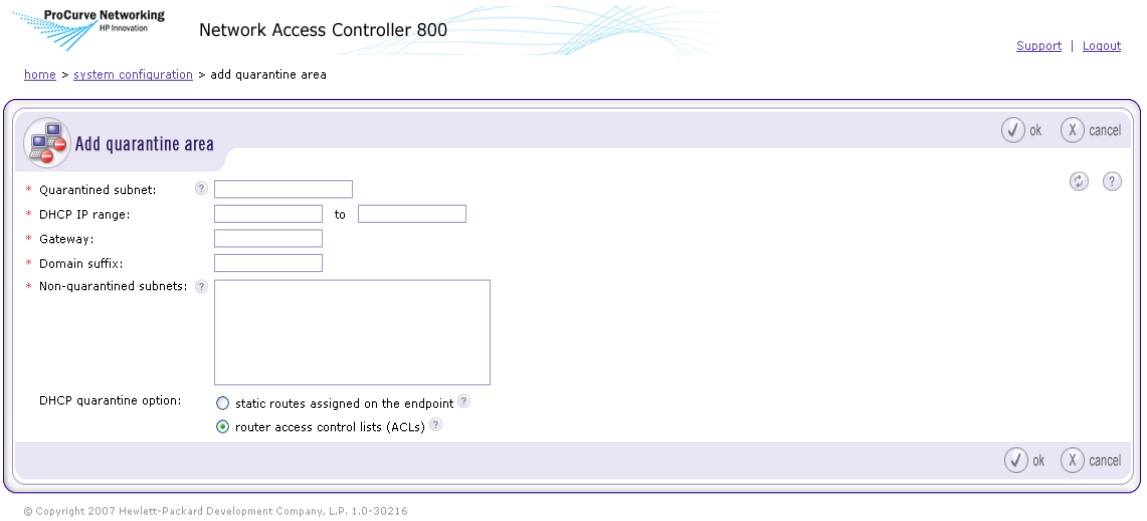


Figure 3-40. Add a Quarantine Area Window

1. In the **Add quarantine area** window, enter the following information:
   - **Quarantined subnet** – The CIDR network that represents the IP space and netmask.
   - **DHCP IP Range** – The start and end DHCP IP addresses to be assigned to quarantined endpoints.
   - **Gateway** – The gateway temporarily assigned to endpoints.
   - **Domain suffix** – The domain name assigned to DHCP clients.
   - **Non-quarantined subnet(s)** – All subnetworks on your LAN except those specified in the quarantined subnet field, separated by a carriage return.

NOTE: The quarantine area subnet(s) and non-quarantined subnet(s) should be entered using Classless Inter-domain Routing address (CIDR) notation (see "Entering Networks Using CIDR Format" on page 13-9).

2. Choose a DHCP quarantine option:
   - **Static routes assigned on the endpoint** – This option restricts the network access of non-compliant endpoints by vending DHCP settings with no gateway and a netmask of 255.255.255.255. Static routes and a Web proxy server built into NAC 800 allow the endpoint access to specific networks, IP addresses, and Web sites. These networks, IP addresses, and Web sites are configured in the accessible endpoint list setting (**System Configuration>>Accessible Services**). The quarantine areas can either be a subset of your existing DHCP scopes or a separate network multinetted on your router.
   - **Router access control lists (ACLs)** – This option restricts the network access of non-compliant endpoints by assigning DHCP settings on a quarantined network. The network, gateway, and ACLs restricting traffic must be configured on your router, which is accomplished by multinetting or adding a virtual interface to the router that acts as the quarantine gateway IP address. The quarantine area DHCP settings must reflect this configuration on your router. The subnets specified in each area must be unique; that is, neither the quarantined nor the non-quarantined subnets in one area can be quarantined or non-quarantined in another.

TIP: The quarantine areas can either be a subset of your existing DHCP scopes or a separate network multinetted on your router. If this option is not selected, enforcement must occur using ACLs on your router.

TIP: To set up multiple quarantine areas, click Add a quarantine area, then enter the information detailed in step 1 for each additional quarantine area.

3. Click **ok**.

Sorting the DHCP Quarantine Area

To sort the quarantine area:

NAC 800 Home window>>System configuration>>Quarantining>>DHCP radio button

1. Click one of the following the column headings to sort the quarantine area by category:
   - **subnet**
   - **dhcp ip range**
   - **gateway**
   - **non-quarantine subnets**
   - **domain suffix**
   - **d** (indicates the quarantine option selected in step 2 on page 3-88)
2. The DHCP quarantine area sorts by the column name clicked.

Editing a DHCP Quarantine Area

To edit a DHCP quarantine area:

NAC 800 Home window>>System configuration>>Quarantining>>DHCP radio button

1. Click **edit** next to the quarantine area you want to edit. The **Quarantine area** window appears:

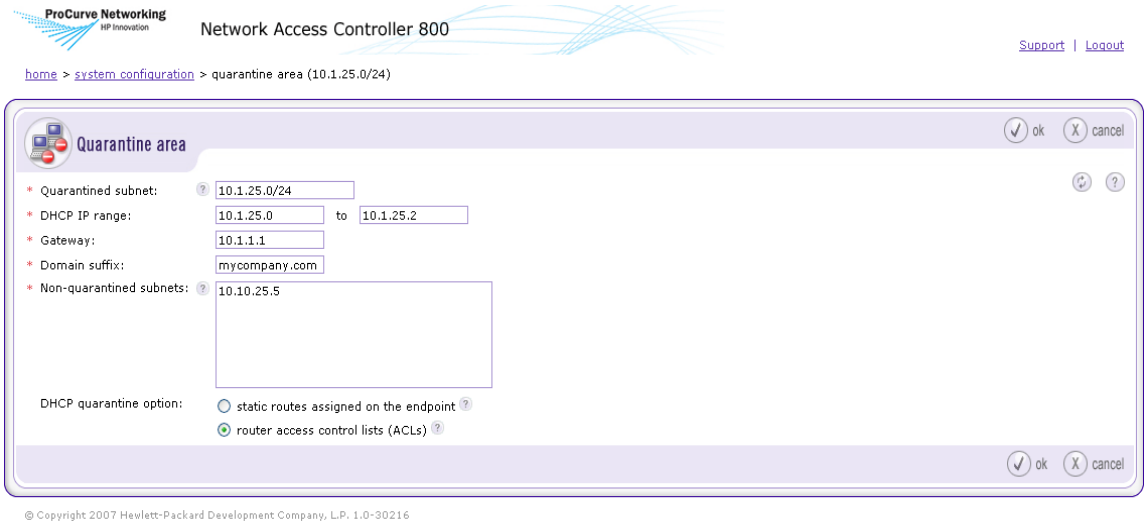


Figure 3-41. Quarantine Area

2. Edit the information in the fields you want to change. See "Adding a DHCP Quarantine Area" on page 3-87 for information on **Quarantine area** options.
3. Click **ok**.

Deleting a DHCP Quarantine Area

To delete a DHCP quarantine area:

NAC 800 Home window>>System configuration>>Quarantining

1. Click **delete** next to the quarantine area you want to remove. The **Delete quarantine area** confirmation window appears
2. Click **yes**.

Maintenance

The **Maintenance** window allows you to back up the MS database, properties files, keystore files, and subscription files in a file with the following name:

`backup-<`*year-month-day*`>Thh-mm-ss.tar.bz2`

where:

- year is the year the system was backed up = 2007
- month is the month the system was backed up = 03
- day is the day the system was backed up = 04
- hh is the hour when the system was backed up = 12
- mm is the minutes when the system was backed up = 11
- ss is the seconds when the system was backed up = 22

For example, a file backed up on March 4, 2007 at 12:11:22 has the following name:

`backup-2007-03-04T12-11-22.tar.bz2`

The following file are backed up:

- Database
- `/usr/local/nac/properties` directory
- `/usr/local/nac/keystore` directory
- `/usr/local/nac/subscription` directory

Initiating a New Backup

To initiate a new backup:

NAC 800 Home window>>System configuration>>Maintenance

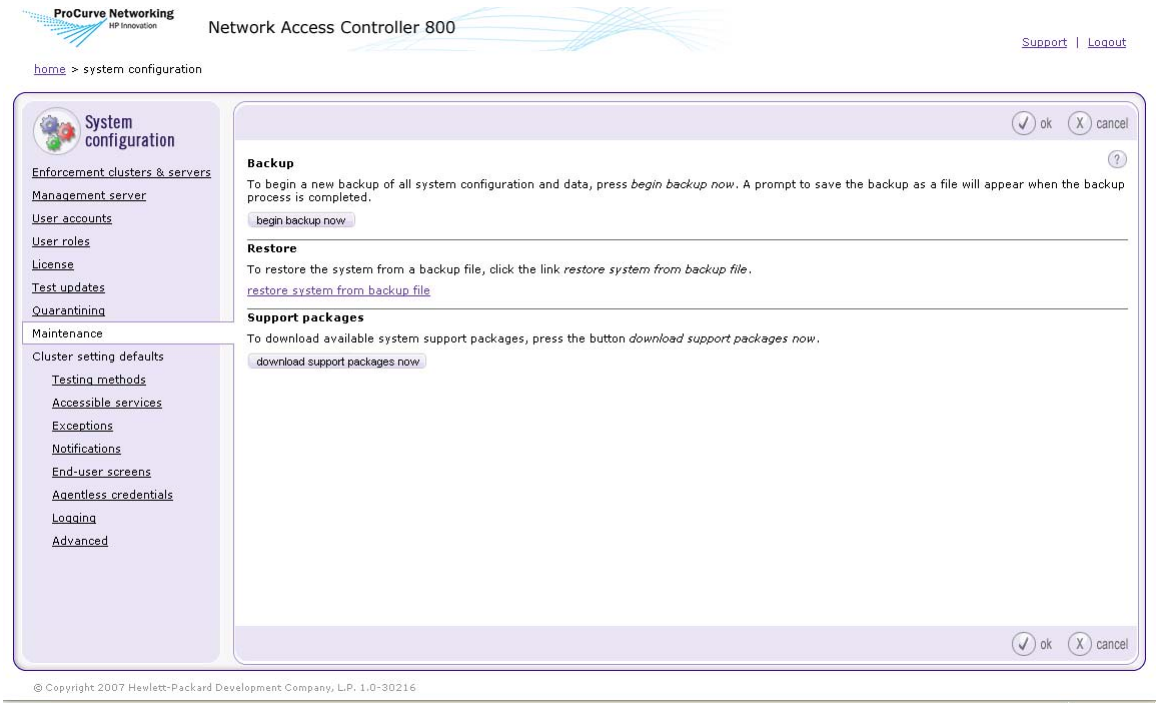


Figure 3-42. System Configuration Window, Maintenance

1. Click **begin backup now** in the **Backup** area. The **Operation in progress** confirmation window appears.
2. A pop-up window appears asking you if you want to save or open the file. Select **Save to disk** and click **OK**. Depending on your browser settings, you might be prompted to select a location for the file.
3. The System b**ackup completed successfully** message appears at the top of the **System configuration** window:

Figure 3-43. Backup Successful Message

Restoring From a Backup

See “Restoring from Backup” on page 13-10 for information about restoring from a backup file.

Downloading Support Packages

Support packages are useful when debugging your system with ProCurve Networking by HP. If a support package is necessary, ProCurve Networking by HP will instruct you to generate one and will provide instructions on how to upload the generated package (a TAR file).

To save a support package to your local computer:

NAC 800 Home window>>System configuration>>Maintenance

1. In the **Support packages** area, click **download support packages now**. A progress window appears.
2. Once the support package is generated, you will be prompted to save the file on your computer. For example, select a directory and click **Save**.

TIP: If you cannot access the GUI, enter the following command at the command line to generate a support package:

generate-support-package.sh

Cluster Setting Defaults

The following sections describe how to globally set the default settings for *all* clusters. For information on overriding the default settings for a specific cluster, see “Enforcement Clusters and Servers” on page 3-6.

Testing Methods

The **Testing methods** menu option allows you to configure the following:

- Select testing methods
- Define order of that the test method screens appear to the end-user
- Select end-user options

Selecting Test Methods

To select test methods:

NAC 800 Home window>>System configuration>>Testing methods

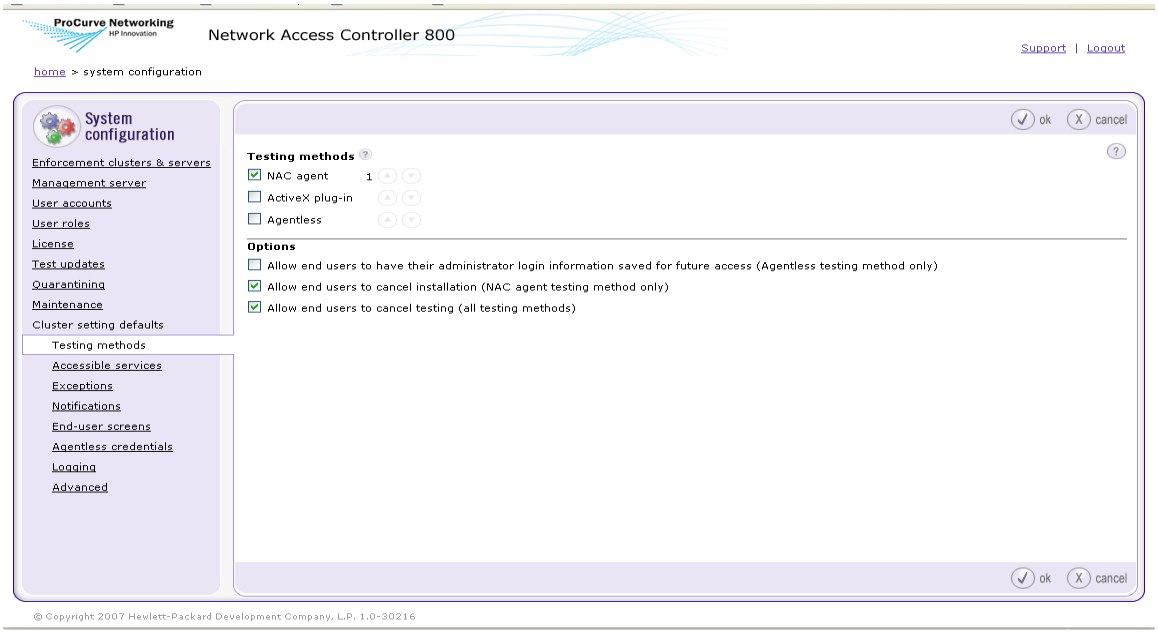


Figure 3-44. System Configuration Window, Testing Methods

1. Select one or more of the following
   a. ProCurve NAC EI Agent – This test method installs a service (ProCurve NAC EI Agent) the first time the user connects.
   b. **ActiveX plug-in** – This test method downloads an ActiveX control each time the user connects to the network. Testing is accomplished through the browser. If the browser window is closed, retesting is not performed.
   c. **Agentless** – This test method uses an existing Windows service (RPC).
2. Click **ok**.

Ordering Test Methods

The NAC 800 backend attempts to test an endpoint transparently in the following order:

1. NAC 800 tries to test with the agent-based test method.
2. If no agent is available, NAC 800 tries to test with the ActiveX test method.

3. If ActiveX is not available and if credentials for the endpoint or domain exist, NAC 800 tries to test with the agentless test method.
4. If the endpoint can not be tested transparently, then NAC 800 uses the end-user access screens to set up a test method and sequence for interacting with the end-user. This order of presentation is defined on the **Testing methods** window.

At least one testing method is required. When testing an endpoint, the end-user screen presented first, is the one that is selected as first here. If this method fails due to a personal firewall or other problem, the second method selected here is presented to the end-user if one has been selected. Finally, if a third method has been selected, it will be presented to the end-user if the second method fails. These system-level settings may be overridden and customized for each cluster.

To order test methods:

NAC 800 Home window>>System configuration>>Testing methods

1. For each test method selected in step 1, Use the arrows next to the testing method name to move the testing methods up or down in the selection order. The order of the testing methods determines the order in which the testing should proceed.
2. Click **ok**.

Recommended Test Methods

Agentless testing is not recommended as the first test method to be used for testing on domains other than your Windows domain for the following reasons:

- Many times guest users do not know the username and password to their machine if they are automatically logged in
- If the end-user is not on a Windows domain they have to change the “Network access... Classic mode” setting
- The user they log in as has to have certain permissions to resources on the system which they may not have
- A guest user may be uncomfortable supplying their Windows username and password to an unknown system

Windows endpoints on your Windows domain are tested automatically when you specify the domain admin credentials in the **System configuration>>Agentless credentials>>Add administrator credentials** window.

Selecting End-user Options

To select end-user options:

NAC 800 Home window>>System configuration>>Testing methods

1. Select one or more of the following options:
   - **Allow end-users to have their administrator login information saved for future access (Agentless testing method only)** – This option allows the end-users to elect to save their login credentials so they do not have to enter them each time they connect.
   - **Allow end-users to cancel installation (agent-based testing method only)** – This option allows end-users to cancel the installation of the agent.
   - **Allow end-users to cancel testing (all testing methods)** – This option allows users to cancel the test process.
2. Click **ok**.

Accessible Services

The **Accessible services** menu option allows you to define which services and endpoints are available to quarantined endpoints.

To define accessible endpoints and services:

NAC 800 Home window>>System configuration>>Accessible services

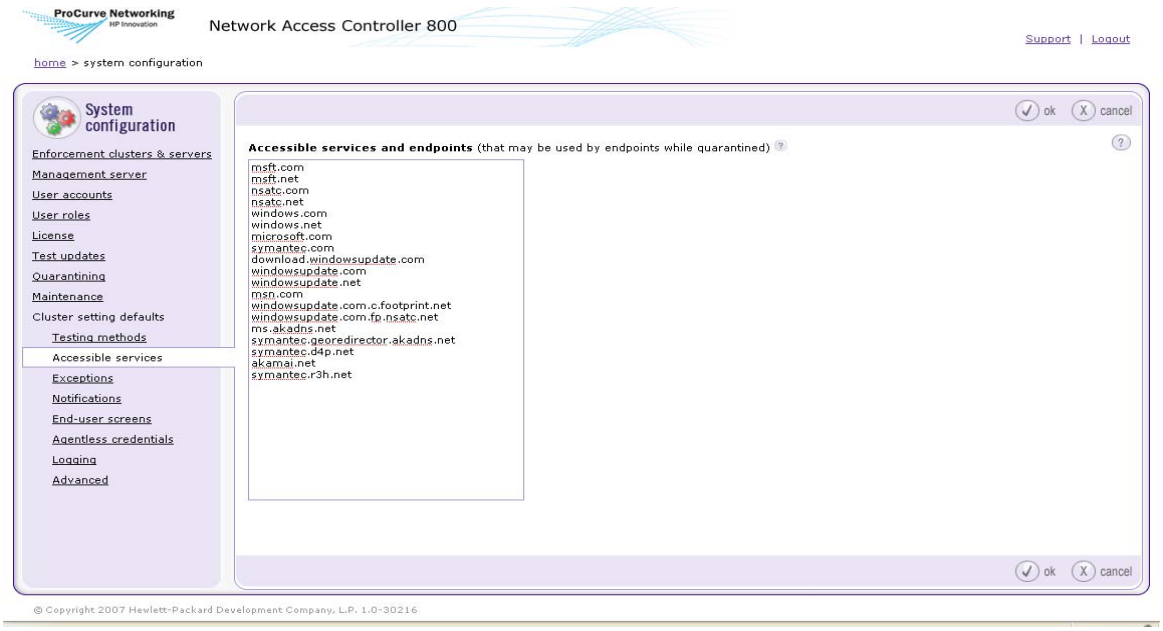


Figure 3-45. System Configuration Window, Accessible Services

1. Enter one or more Web sites, host names, IP addresses, ports, endpoints, or networks, that are accessible to connecting endpoints when they fail their compliance tests. You can enter these endpoints and services in the following formats separated by a carriage return. Enter a range of IPs with a dash (-) between the IPs, or use CIDR addresses. You might also need to specify the DHCP server IP address in this field. If the Domains connection method is enabled (**System Configuration>>Quarantining>>802.1X>>Windows domain End-user authentication method**), you must specify your Windows domain controller.

   Examples:

   Web sites – `www.mycompany.com`
   Host names – `bagle.com`
   IP addresses – `10.0.16.100`
   Ports – `10.0.16.100:53`
   Networks – `10.0.16.1/24`
   Range of IP addresses – `10.0.16.1-10.0.16.5`

   You do not need to enter the IP address of the NAC 800 server here. If you

do, it can cause redirection problems when end-users try to connect. You do need to add any update server names, such as the ones that provide anti-virus and software updates. NAC 800 ships with many of the default server names pre-populated, such as `windowsupdate.com`.

2. Click **ok**.

The following table provides additional information about accessible services and endpoints.

Topic	Tip
Modes and IP addresses	When using inline mode, enter IP addresses rather than domain names. When using DHCP mode, use domain names for sites the user needs to access, such as update servers, and use IP addresses for endpoints that sit behind NAC 800, such as authentication servers.
Ranges	Use a hyphen for a range of IP addresses (10.0.16.1 to 10.0.16.5) and a colon for a range of ports (10.0.16.1:80:90).
DHCP server IP address	In inline mode, you might need to specify the DHCP server IP address in this field.
Domain controller name	Regardless of where the Domain Controller (DC) is installed, you must specify the DC name on the Quarantine tab in the Quarantine area domain suffix field for each quarantine area defined.
DHCP server and Domain controller	In DHCP mode, when your DHCP server and Domain Controller are behind NAC 800, you must specify ports 88, 135 to 159, 389, 1025, 1026, and 3268 as part of the address. If you do not specify a DHCP address, users are blocked. If you specify only the IP address with no port, endpoints are not quarantined, even for failed tests. If your domain controller is not situated behind NAC 800, you must configure your router to allow routes from the quarantine area to your domain controller on ports 88, 135-159, 389, 1025, 1026, and 3268.
Windows update server	In inline mode, if an endpoint is quarantined and needs to access the Windows Update server, it is not able to unless you enter `207.46.0.0/16` here. This is because iptables needs an IP address, and would not be able to resolve the default of `windowsupdate.com`.

Table 3-4.Accessible Services and Endpoints Tips

Exceptions

The Exceptions menu option allows you to define the following:

- The endpoints and domains that are always allowed access

- The endpoints and domains that are always quarantined

Always Granting Access to Endpoints and Domains

To always grant access to endpoints and domains:

NAC 800 Home window>>System configuration>>Exceptions

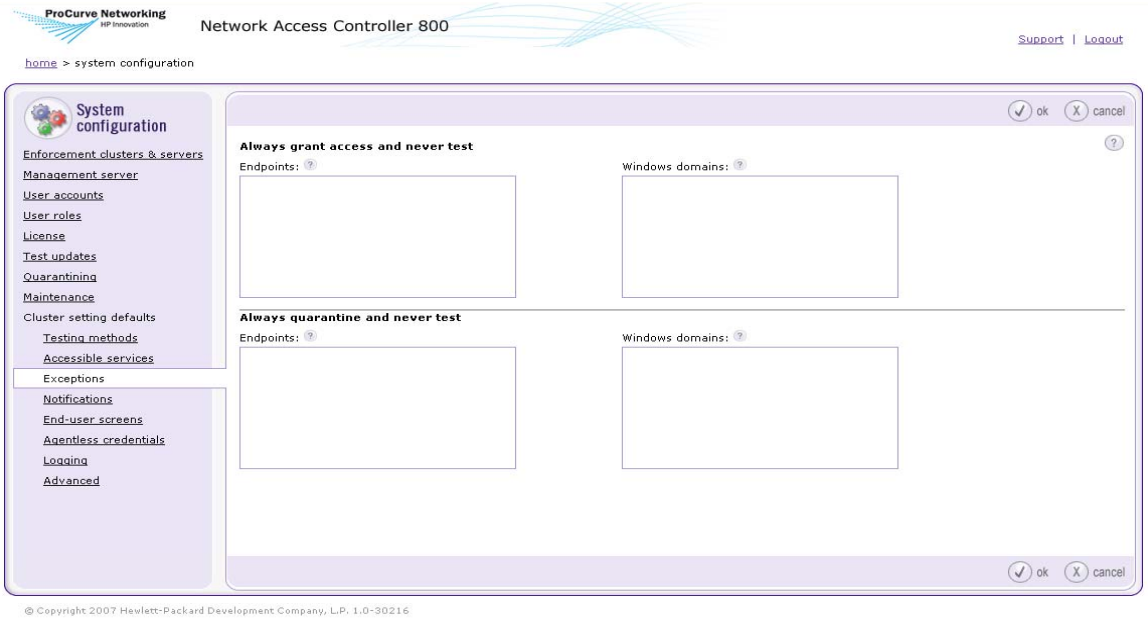


Figure 3-46. System Configuration, Exceptions

1. To exempt endpoints from testing, in the **Always grant access and never test** area, enter the endpoint(s) by MAC or IP address, or NetBIOS name.
2. To exempt end-user domains from testing, in the **Always grant access and never test** area, enter the domain names.
3. Click **ok**.

CAUTION:

If you enter the same endpoint in both the Always grant access and never test and the Always quarantine and never test areas in the Exceptions window, the Always grant access and never test option is used.

Always Quarantine Endpoints and Domains

To always quarantine endpoints and domains:

NAC 800 Home window>>System configuration>>Exceptions

1. To always quarantine endpoint(s) when testing, in the **Always quarantine and never test** area, enter the endpoint(s) by MAC or IP address, or NetBIOS name.
2. To always quarantine domain(s) when testing, in the **Always quarantine and never test** area, enter the domain(s).

TIP: In DHCP mode, the NAC 800 firewall quarantines based on MAC address (everything entered must be translated to the corresponding endpoint's MAC address). This translation occurs each time activity from the endpoint is detected. To reduce translation time, use the MAC address initially.

CAUTION: If you enter the same endpoint in both the Always grant access and never test and the Always quarantine and never test areas in the Exceptions window, the Always grant access and never test option is used.

Notifications

The **Notifications** menu option allows you to configure email notifications sent to announce test alerts and system errors. You can configure the following:

- Send email notifications
- Elect not to send notifications

Enabling Notifications

To enable email notifications:

NAC 800 Home window>>System configuration>>Notifications

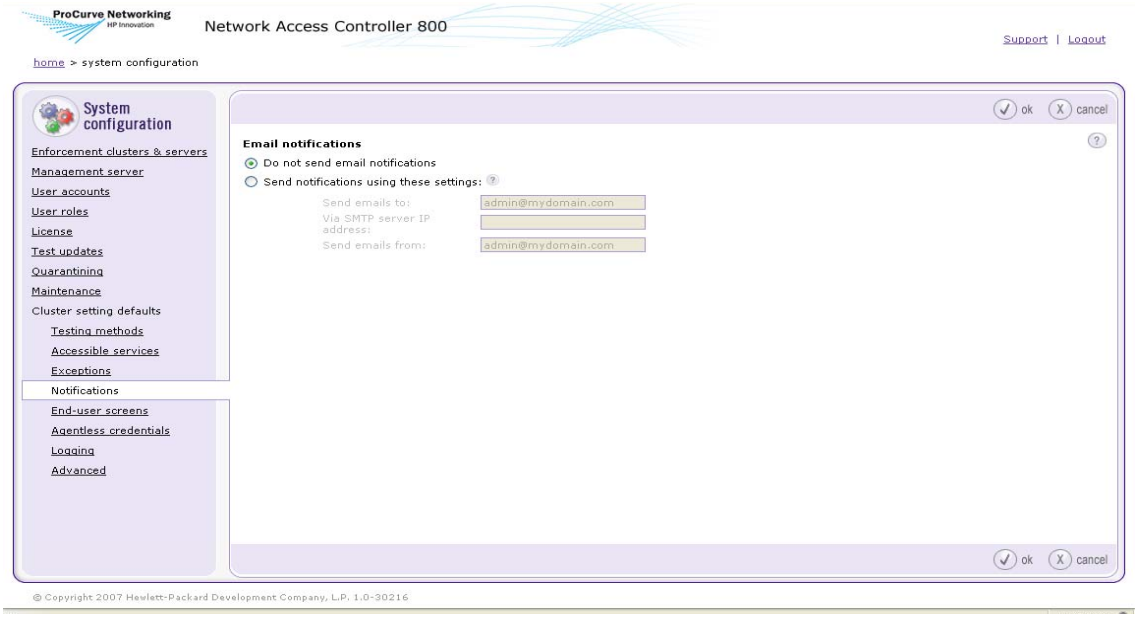


Figure 3-47. System Configuration, Notifications

1. To send email notifications, you must provide NAC 800 with the IP address of a Simple Mail Transfer Protocol (SMTP) email server. This SMTP email server must allow SMTP messages from the NAC 800 machine. Use the following steps to configure the SMTP email server function:
   a. Select the radio button next to **Send email notifications**.
   b. In the **Send emails to** text box, enter the email address of the person or group (alias) who should receive the notifications.
   c. In the **Via SMTP server IP address** text box, enter the IP address of the SMTP email server from which NAC 800 sends email notifications. This must be a valid IP address that is reachable from where the NAC 800 machine is located on your network.
   d. In the **Send emails from** text box, enter the email address from which notifications should originate. You might have to enter a valid email address (for example, one within your organization) for the SMTP email server to send notifications.
2. Click **ok**.

To disable email notifications:

NAC 800 Home window>>System configuration

1. Select a cluster. The **Enforcement cluster** window appears.
2. Select the **Notifications** menu item.
3. Select the **For this cluster, override the default settings** check box.
4. Select **Do not send email notifications**.
5. Click **ok**.

End-user Screens

The **End-user screens** menu option allows you to configure the end-user screens with the following:

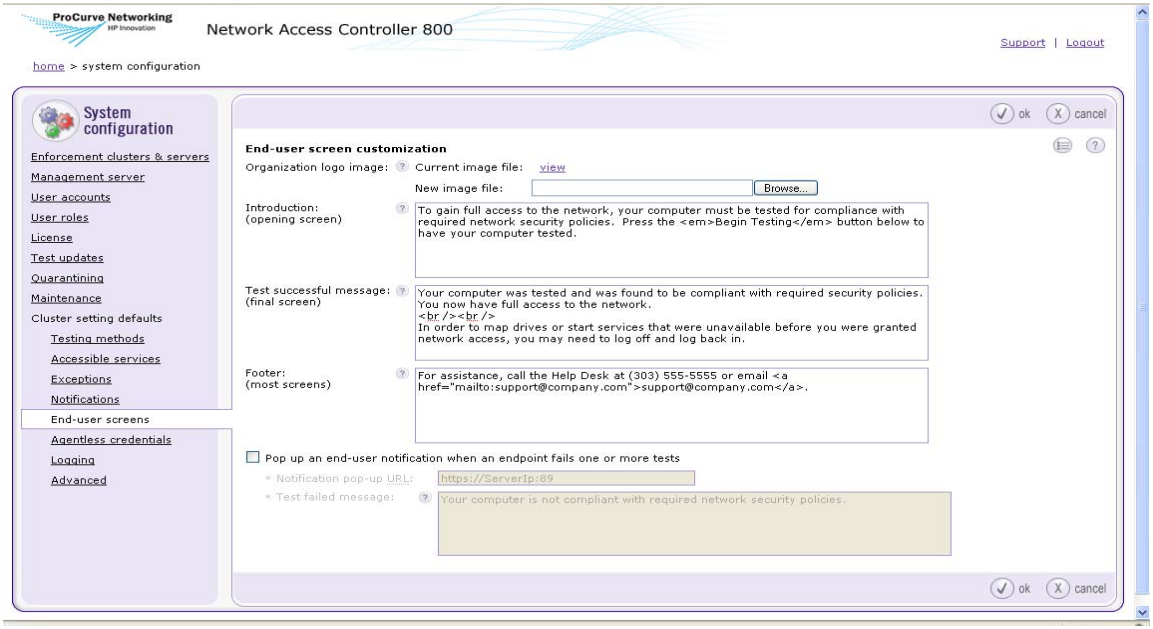
- Define logo image to be displayed
- Specify text to be displayed on end-user screens
- Optionally define a pop-up window as an end-user notification when an endpoint fails one or more tests

The end-user screens are shown in "End-user Access" on page 5-1.

Specifying an End-user Screen Logo

To specify an end-user screen logo:

NAC 800 Home window>>System configuration>>End-user screens


ProCurve Networking
HP Innovation
Network Access Controller 800
Support | Logout
home > system configuration
System configuration
Enforcement clusters & servers
Management server
User accounts
User roles
License
Test updates
Quarantining
Maintenance
Cluster setting defaults
Testing methods
Accessible services
Exceptions
Notifications
End-user screens
Agentless credentials
Logging
Advanced
ok
cancel
End-user screen customization
Organization logo image:
Current image file:
view
New image file:
Browse...
Introduction:
(opening screen)
To gain full access to the network, your computer must be tested for compliance with required network security policies. Press the Begin Testing button below to have your computer tested.
Test successful message:
(final screen)
Your computer was tested and was found to be compliant with required security policies. You now have full access to the network.

In order to map drives or start services that were unavailable before you were granted network access, you may need to log off and log back in.
Footer:
(most screens)
For assistance, call the Help Desk at (303) 555-5555 or email support@company.com.
Pop up an end-user notification when an endpoint fails one or more tests
* Notification pop-up URL:
https://Server1p:89
* Test failed message:
Your computer is not compliant with required network security policies.
ok
cancel

Figure 3-48. System Configuration Window, End-user Screens

1. Enter the customization information:

   Organization logo image – Enter a path to your organization's logo, or click **Browse** to select a file on your network. ProCurve recommends you place your logo here to help end-users feel secure about having their computers tested. The logo should be no larger than 450x50 pixels.

2. Click **ok**.

Specifying the End-user Screen Text

To specify the end-user screen text:

NAC 800 Home window>>System configuration>>End-user screens

1. Enter the customization information:
   a. **Introduction (opening screen)** – Enter the introduction text for the default window. ProCurve recommends you provide text here that sets the stage for the end-user's experience.

b. **Test successful message (final screen)** – Enter the text for the final, test successful window. ProCurve recommends that this text informs the end-user that the test was successful and provides any additional helpful information such as instructions, notices, and so on.

c. **Footer (most screens)** – Enter the text for the footer that appears on most of the end-user windows. ProCurve recommends that this text includes a way to contact you if they need further assistance. You can format the text in this field with HTML characters.

2. Click **ok**.

Specifying the End-user Test Failed Pop-up Window

To specify the end-user test failed pop-up window:

NAC 800 Home window>>System configuration>>End-user screens

1. Select the **Pop up an end-user notification when an endpoint fails one or more tests** check box to turn the pop-up window on (clear the check box to turn it off).
2. Enter the customization information:
   a. **Notification pop-up URL** – In the **Notification pop-up URL** text box, the default is:

      ```
      https://ServerIpaddress:89
      ```

      This URL points to port 89 on the NAC 800 ES (the default end-user screen that shows the test failed results), and is where the user is directed to when they click the **Get details** button on the new pop-up window.

TIP: Enter a different URL if you have a custom window you want the users to see. For example, you might have a location that provides links to patch or upgrade their software.

   b. **Test failed pop-up message** – In the **Test failed pop-up message** text box, enter the message the end-user views on the standard pop-up window.

TIP: You can verify your changes to the end-user access screens immediately by pointing a browser window to port 88 of your NAC 800 installation. For example, if the IP address of your NAC 800 installation is 10.0.16.18, point the

browser window to:

http://10.0.16.18:88

3. Click **ok**.

Agentless Credentials

When NAC 800 accesses and tests endpoints, it needs to know the administrator credentials for that endpoint. If your network uses a Windows domain controller and the connecting endpoint is a member of a configured domain, NAC 800 uses the information supplied to access and test the endpoint.

TIP: Setting windows credentials here sets them as default settings for all clusters. You can override these settings on a per-cluster basis by selecting a cluster first, and then making changes in Agentless credentials.

Adding Windows Credentials

To add Windows credentials:

NAC 800 Home window>>System configuration>>Agentless credentials

Figure 3-49. System Configuration Window, Agentless Credentials

1. Click **Add administrator credentials**. The **Add Windows administrator credentials** window appears:

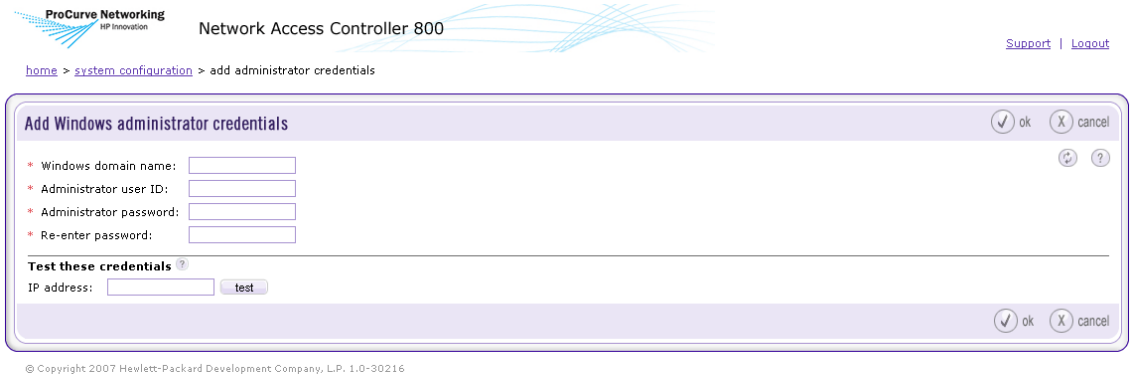


Figure 3-50. Agentless Credentials, Add Windows Administrator Credentials Window

2. In the **Add Windows administrator credentials** window, enter the following:

- **Windows domain name** – Enter the domain name of the Windows machine, for example: mycompanyname. You can also enter a group name, for example: WORKGROUP or HOME.
- **Administrator user ID** – Enter the administrator login name of the Windows machine, for example: `jsmith`.
- **Administrator password** – Enter the password for the administrator login name used in the ID text field.

3. Click **ok**.

Testing Windows Credentials

To test Windows credentials:

NAC 800 Home window>>System configuration>>Agentless credentials

1. In the **Test these credentials** area, enter the IP address of the endpoint.

TIP: When using a multi-server installation, the credentials are stored on the ES, but the test is initiated from the MS. You will need to have a route identified between the MS and the ES in order for this test to work.

2. Click **test**. The operation in progress window appears. Testing the credentials might take a few minutes to complete.
3. When the credentials testing is complete, the test status is displayed at the top of the credentials window.

NOTE: NAC 800 saves authentication information encrypted on the NAC 800 server. When a user connects with the same browser, NAC 800 looks up this information and uses it for testing.

TIP: When using the Windows administrator account connection method, NAC 800 performs some user-based tests with the administrator account's user registry settings, rather than those of the actual user logged into the endpoint. This only affects Internet Explorer security tests, MS Office Macro Settings tests, and individual user's Windows startup settings.

Editing Windows Credentials

To edit Windows credentials:

NAC 800 Home window>>System configuration>>Agentless credentials

1. Click **edit** next to the name of the Windows administrator credentials you want to edit.
2. Enter or change information in the fields you want to change. (See “Adding Windows Credentials” on page 3-107 for more information about Windows administrator credentials.
3. Click **ok**.

Deleting Windows Credentials

To delete Windows credentials:

NAC 800 Home window>>System configuration>>Agentless credentials

1. Click **delete** next to the name of the Windows administrator credentials you want to remove. The **Delete Windows administrative credentials** conformation window appears.
2. Click **yes**.

Sorting the Windows Credentials Area

To sort the Windows credentials area:

NAC 800 Home window>>System configuration>>Agentless credentials

1. Sort the Windows administrator credentials by clicking on a column heading.
2. Click **ok**.

Logging

Setting ES Logging Levels

You can configure the amount of diagnostic information written to log files, ranging from error (error-level messages only) to trace (everything).

To set ES logging levels:

NAC 800 home window>>System configuration>>Logging

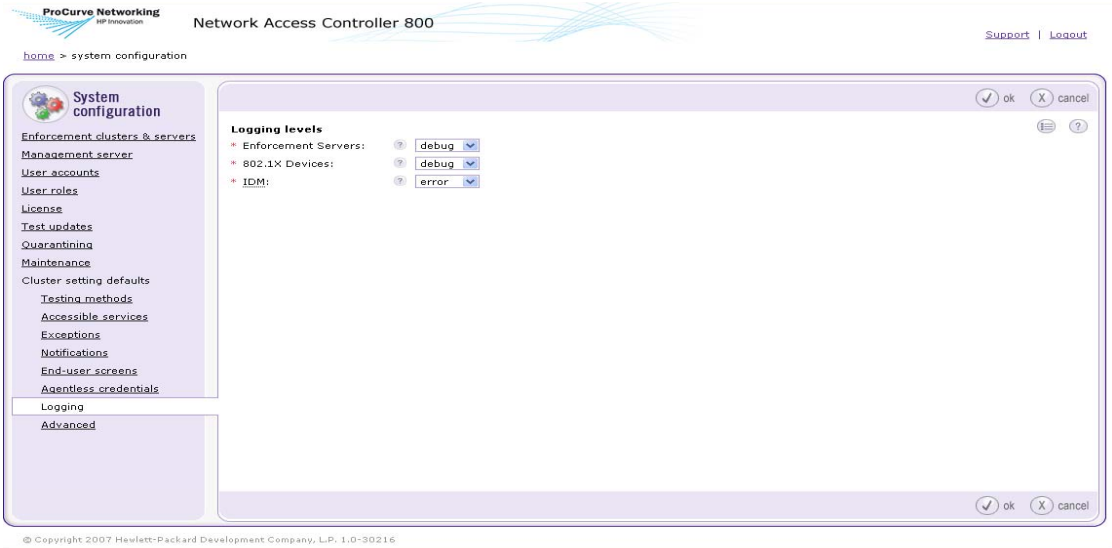


Figure 3-51. System Configuration Window, Logging Option

1. To configure the amount of diagnostic information written to log files, select a logging level from the **Enforcement servers** drop-down list:
   - error – log error-level messages only
   - warn – log warning-level and above messages only
   - info – log info-level messages and above only
   - debug – log debug-level and above messages only
   - trace – log everything

CAUTION: Setting the log level to trace may adversely affect performance.

2. Click **ok**.

Setting 802.1X Devices Logging Levels

You can configure the amount of diagnostic information written to log files related to 802.1X re-authentication, ranging from error (error-level messages only) to trace (everything).

To set 802.1X logging levels:

NAC 800 home window>>System configuration>>Logging

1. To configure the amount of diagnostic information written to log files related to 802.1X re-authentication, select a logging level from the **802.1X devices** drop-down list:
   - error – log error-level messages only
   - warn – log warning-level and above messages only
   - info – log info-level and above messages only
   - debug – log debug-level and above messages only
   - trace – log everything

CAUTION: Setting the log level to trace may adversely affect performance.

2. Click **ok**.

Setting IDM Logging Levels

You can configure the amount of diagnostic information written to log files related to IDM, ranging from error (error-level messages only) to trace (everything).

To set IDM logging levels:

NAC 800 home window>>System configuration>>Logging

1. To configure the amount of diagnostic information written to log files related to IDM, select a logging level from the **IDM** drop-down list:
   - error – log error-level messages only
   - warn – log warning-level messages only

- info – log info-level messages only
- debug – log debug-level messages only
- trace – log everything

CAUTION: Setting the log level to trace may adversely affect performance.

2. Click **ok**.

Advanced Settings

This section describes setting the timeout periods. Endpoint detection is described in “Working with Ranges” on page 13-39.

Setting the Agent Read Timeout

To set the Agent read timeout period:

NAC 800 home window>>System configuration>>Advanced

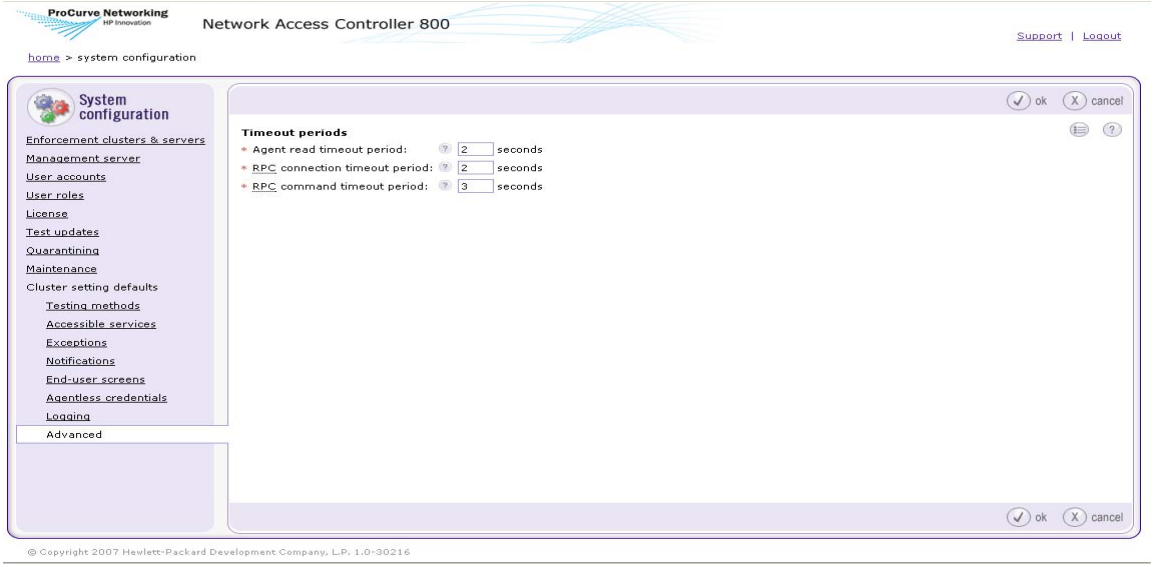


Figure 3-52. System Configuration Window, Advanced Option

1. Enter a number of seconds in the **Agent read timeout period** text field. The agent read time is the time in seconds that NAC 800 waits on an agent read. Use a larger number for systems with network latency issues.
2. Click **ok**.

Setting the RPC Connection Timeout

To set the RPC connection timeout period:

NAC 800 home window>>System configuration>>Advanced

1. Enter a number of seconds in the **RPC connection timeout period** text field. The RPC connection timeout is the time in seconds that NAC 800 waits on a connection to the RPC port. Use a larger number for systems with network latency issues.
2. Click **ok**.

Setting the RPC Command Timeout

To set the RPC command timeout period:

NAC 800 home window>>System configuration>>Advanced

1. Enter a number of seconds in the **RPC command timeout period** text field. The RPC command timeout is the time in seconds that NAC 800 waits on an `rpcclient` command to finish. Use a larger number for systems with network latency issues.
2. Click **ok**.

(This page intentionally left blank.)

Endpoint Activity

Chapter Contents

Overview 4-2
Filtering the Endpoint Activity Window 4-4
Filtering by Access Control or Test Status 4-4
Filtering by Time 4-5
Limiting Number of Endpoints Displayed 4-6
Searching 4-7
Access Control States 4-9
Test Status States 4-10
Selecting Endpoints to Act on 4-15
Acting on Selected Endpoints 4-16
Manually Retest an Endpoint 4-16
Immediately Grant Access to an Endpoint 4-16
Immediately Quarantine an Endpoint 4-17
Clearing Temporary Endpoint States 4-17
Viewing Endpoint Information 4-18

Overview

Use the **Endpoint activity** window, to monitor end-user connection activity.

NAC 800 Home window>>Endpoint activity

The **Endpoint activity** window has the following sections:

- Endpoint selection area – The left column of the window provides links that allow you to quickly filter the results area by **Access control status** or **Endpoint test status**.
- Search criteria area – The top right area of the window allows you to filter the results by cluster, NetBIOS name, IP address, MAC address, User ID, domain, NAC policy, operating system, and time.
- Search results area – The lower right area of the window displays the combined results of the selection made in the left column and the search criteria entered in the top portion of the window.

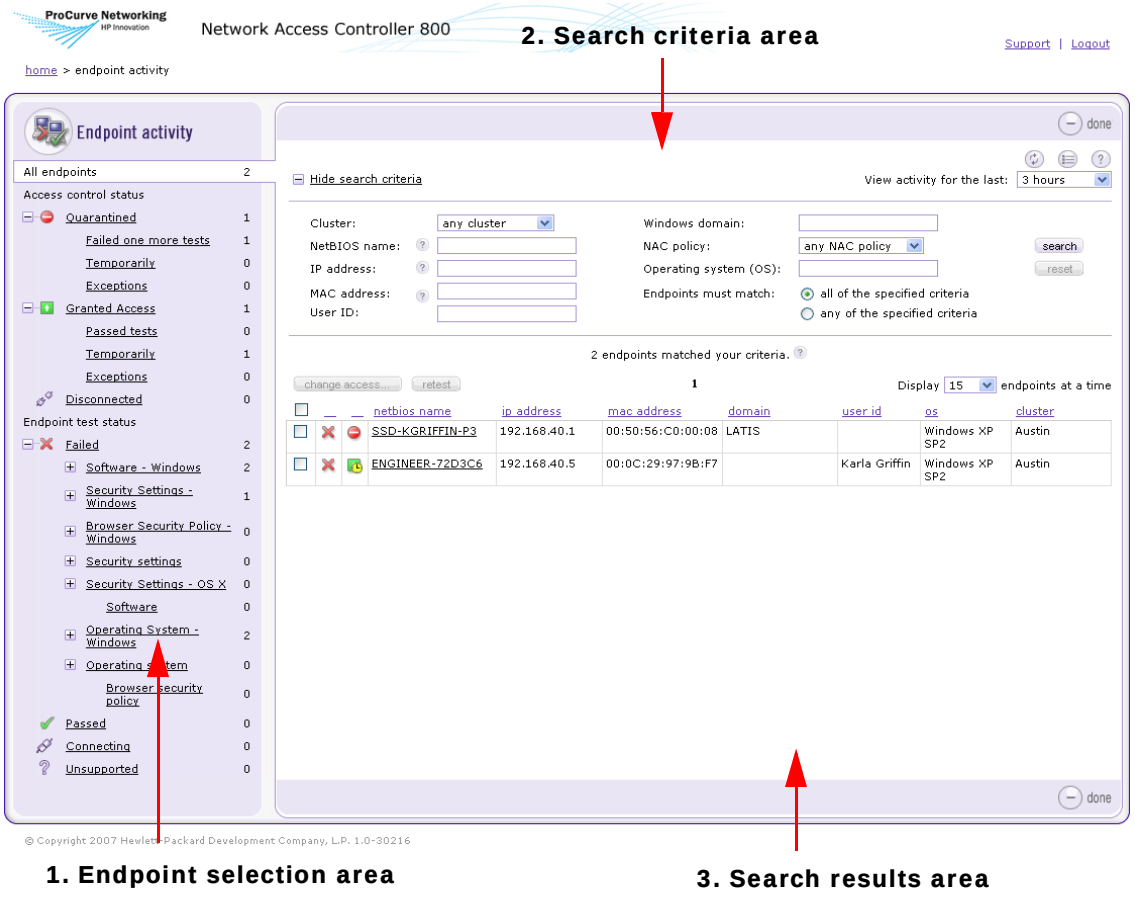


Figure 4-1. Endpoint Activity, All Endpoints Area

Filtering the Endpoint Activity Window

You can modify the results shown in the **Endpoint activity** window to include activity for the following:

- Access control status
- Endpoint test status
- Configurable time frame
- Cluster
- NetBIOS name
- IP address
- MAC address
- User ID
- Windows domain
- NAC policy
- Operating system
- Number of endpoints to display

Filtering by Access Control or Test Status

NAC 800 Home window>>Endpoint activity window

Select a method for filtering the results window; by a specific access control status or endpoint status as shown in the following figure:

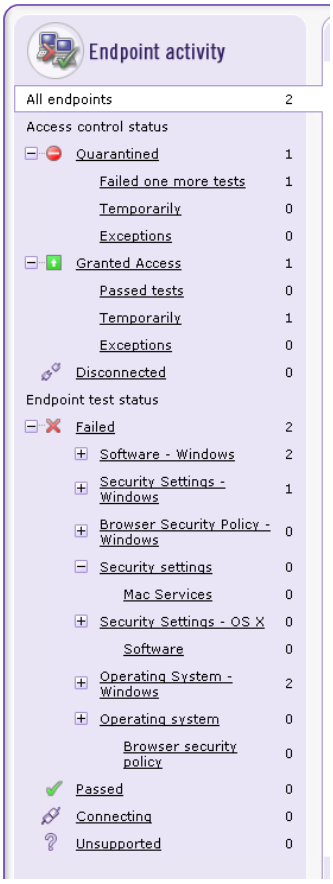


Figure 4-2. Endpoint Activity, Menu Options

Filtering by Time

To filter the information displayed:

NAC 800 Home window>>Endpoint Activity

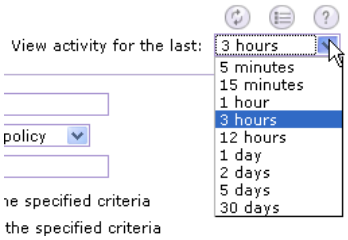


Figure 4-3. View Activity for the Last Drop-down List

The **View activity for the last** drop-down list is a high-level filter that drives all the information displayed. All the information in the **Endpoint activity** window pertains only to the selected time.

Select one of the options from the drop-down list; the results area updates to match the time frame selected.

Limiting Number of Endpoints Displayed

To limit the number of endpoints displayed:

NAC 800 Home window>>Endpoint Activity

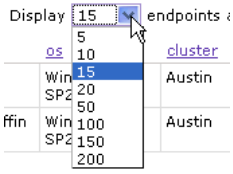


Figure 4-4. Display Endpoints Drop-down

Select a number from the drop down list. The results area updates to show only the number of endpoints selected with page navigation links as shown in the following figure:

Figure 4-5. Endpoint Activity Page Navigation Links

Searching

To search the **Endpoint activity** window.

NAC 800 Home window>>Endpoint activity>>Search criteria area

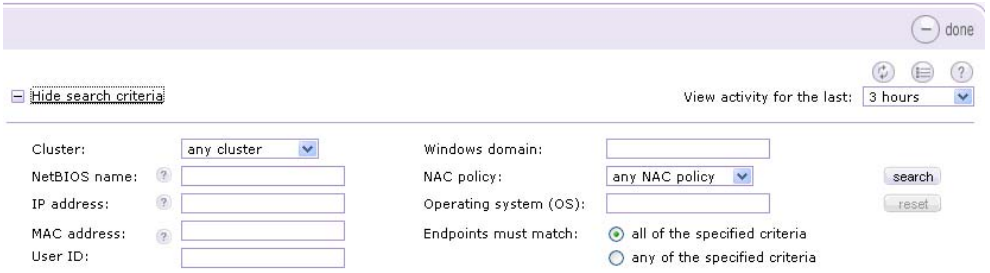


Figure 4-6. Search Criteria Window

1. Select a **Cluster** or **NAC policy** from the drop-down lists and enter any text string in one of the text boxes you want to search for (you can leave these blank).
2. Select either the **Endpoints must match all of the specified criteria** or the **Endpoints must match any of the specified criteria** radio button.
3. Click **Search**. The results area updates to match the search criteria specified.
4. To refresh the **Endpoint activity** window with all activity, click **Reset**.

TIP: The search box is not case-sensitive. Searching matches entire words. You must enter wildcard characters (*) to match substrings. For example, 192.168.*.

Access Control States

NAC 800 provides on-going feedback on the access status of endpoints as follows:

TIP: To view access status, see "Viewing Endpoint Access Status" on page 4-14.

- Quarantined – The endpoint has been assigned a quarantined IP address. For example, an endpoint could have been quarantined because it failed a test or it could not be tested.
- Quarantined by exception – The endpoint has been assigned a quarantined IP address because it was designated to always be quarantined on the **System Configuration>>Tests** window.
- Temporarily quarantined until XX/XX/XX at HH:MM pm – The administrator has selected **Quarantine for** and assigned a time frame.
- Granted access – The endpoint has been assigned a non-quarantined IP address. For example, an endpoint could have access because it passed a test, could not be tested but is allowed access.
- Granted access by exception – The endpoint has been assigned a non-quarantined IP address because it was designated to always have access in the **System Configuration>>Tests** window
- Has temporary access until XX/XX/XX at HH:MM pm (by admin) – The endpoint has been given temporary access by the administrator.
- Has temporary access until XX/XX/XX at HH:MM pm (by NAC policy) – The endpoint has been given temporary access by an NAC policy.
- Disconnected – NAC 800 cannot communicate with the endpoint.
- Error – This is most likely a problem that cannot be resolved without contacting ProCurve. Try to force a retest from the NAC 800 console. If that does not work, call ProCurve Networking by HP and be prepared to generate a support package (see "Generating a Support Package" on page 13-11).

Test Status States

NAC 800 provides on-going feedback on the test status of endpoints as follows:

TIP: To view access status, see "Viewing Endpoint Access Status" on page 4-14.

- Unknown error – This is most likely a problem that cannot be resolved without contacting ProCurve. Try to force a retest from the NAC 800 console. If that does not work, call ProCurve Networking by HP and be prepared to generate a support package (see "Generating a Support Package" on page 13-11).
- Connecting – NAC 800 shows this status briefly after the endpoint has been tested while the endpoint is being assigned a non-quarantined IP address.
- Awaiting credentials – NAC 800 shows this status briefly while the agentless credentials (Windows, LDAP, or RDBMS) are being verified.
- Bad credentials – NAC 800 shows this status when the agentless credentials could not be verified. The end-user is presented with a window stating why the credentials may have failed, and is given the opportunity to re-enter the credentials, cancel the test, or try the next test method (specified on the **End-user access** window).
- Testing (agentless test) – NAC 800 shows this status briefly while the agentless test is being performed.
- Pass – NAC 800 shows this status after the endpoint has passed the test and is connected to the network.
- Fail – NAC 800 shows this status after the endpoint has failed testing.
- Could not be tested – NAC 800 shows this status after the endpoint could not be tested.
- License limit exceeded – NAC 800 shows this status when the number of endpoints allowed on your license has been exceeded. The endpoint is not tested or allowed access.
- License expired – NAC 800 shows this status when your license has expired. No endpoints are tested or allowed access to the network.
- Test canceled – NAC 800 shows this status when the end-user cancels the test.

- Access always allowed – NAC 800 shows this status when an endpoint has been listed in the **System configuration>>Exceptions** window to always grant access. These endpoints are never tested and always allowed access.
- Access always quarantined – NAC 800 shows this status when an endpoint has been listed in the **System configuration>>Exceptions** window to always quarantine. These endpoints are never tested and always quarantined.
- Awaiting test initiation – NAC 800 shows this status when one of the following conditions occurs:
  - NAC 800 doesn't have credentials and there is no agent
  - NAC 800 doesn't have credentials and the endpoint is firewalled
  - NAC 800 is waiting for credentials or an agent
  - No testing has taken place yet
- Installing test service – NAC 800 shows this status briefly while the agent is being installed.
- Install canceled – NAC 800 shows this status when the end-user has cancelled the installation of the agent.
- Testing (installed test) – NAC 800 shows this status briefly while the endpoint is being tested by the agent-based method.
- Testing (one-time test) – NAC 800 shows this status briefly while the endpoint is being tested by the ActiveX method.
- Installing one-time plug-in – NAC 800 shows this status briefly while the ActiveX plug-in is being installed .
- One-time plug-in installation failed – NAC 800 shows this status when installation of the ActiveX plug-in failed. The installation probably failed due to browser settings (see “Important Browser Settings” on page B-1). The end-user has the option to retry or cancel which presents the user with the next testing method specified on the **End-user access** screen.
- Validating install – NAC 800 shows this status while NAC 800 is validating that the agent is working.
- Install failed – NAC 800 shows this status when the agent cannot be installed. This is likely due to permission problems on the endpoint.
- Agent not active – NAC 800 shows this status when an endpoint that was previously running the agent is no longer running the agent. This is likely due to a firewall being turned on.

- Awaiting ip transition – NAC 800 shows this status during a transition from a quarantined IP address and a non-quarantined IP address and vice versa.
- Connection failed - endpoint busy or file and print sharing disabled – During the connection to the endpoint, the endpoint is not able to complete the requested testing by NAC 800. This condition can occur when then endpoint is busy running other processes or programs, or it might be in an overloaded condition. Retesting the endpoint again at a later time generally resolves this problem. Defragmenting the hard disk can also help this situation on slower endpoints.
- Connection failed - unsigned SMB – NAC 800 is not able to connect to the endpoint as it only allows signed connections to Windows SMB services. This generally occurs on endpoints running Windows 2003 Server. To resolve this problem, configure the endpoint to allow unsigned SMB connections and then retest the endpoint. Alternatively, the NAC Agent or ActiveX browser plug-in can be used to test the endpoint.
- Connection failed - no logon server – During the connection process, the endpoint was not able to validate the user ID and password credentials supplied by NAC 800 because the endpoint does not have network access to any authentication servers. This can be due to a routing issue which is not allowing the endpoint to reach the necessary servers on the network. Also, if NAC 800 is inline with the domain controller, you might need to open up the appropriate ports (135 through 138, 445, 389, 1029) in the NAC 800 accessible endpoints configuration for your domain controller IP address. Once the endpoint can reach the necessary server(s), retest the endpoint.
- Connection failed - endpoint/domain trust failure – The supplied credentials failed to authenticate because a previous trust relationship established between the endpoint and the Windows directory is broken in some way. Resolve this problem by adding the endpoint again as a member of the appropriate Windows domain, then retest the endpoint.
- Connection failed - timed out – NAC 800 timed out while trying to connect to or retrieve information from the endpoint. This could be due to a slow or saturated network, or the endpoint might have been shutdown or rebooted while it was being tested by NAC 800. If the endpoint is still on the network, retest it with NAC 800.
- Connection failed - session setup – NAC 800 shows this status when the RPC client had problems communicating with the endpoint.

- Test failed - insufficient test privileges – The credentials NAC 800 used to test the endpoint do not have sufficient privileges to read the registry or enumerate the services. An easy way to debug this is to run `regedit` and connect to the remote endpoint using the same admin credentials supplied to NAC 800. You should be allowed to browse the HKLM\Software and HKLM\System keys on the endpoint. Retest the end point after increasing the credential permission levels or using a different set of credentials with the necessary permissions.
- Connection failed - no route to host – The endpoint is unreachable on the network by NAC 800. This can be due to either a network routing issue or because the endpoint has powered off or is in the process of rebooting. Retest the endpoint once the routing issues have been resolved or the endpoint is back on the network.
- Endpoint disconnected before could be tested – NAC 800 shows this status when the endpoint disconnects from the network before testing could be completed.

Viewing Endpoint Access Status

To view access status for a endpoint:

NAC 800 Home window>>Endpoint activity window

1. Locate the endpoint you are interested in.
2. The first column is the selection column, the second column is the **Endpoint test status** column, and the third column is the **Access control status** column. The icons shown in the following figure provide status:

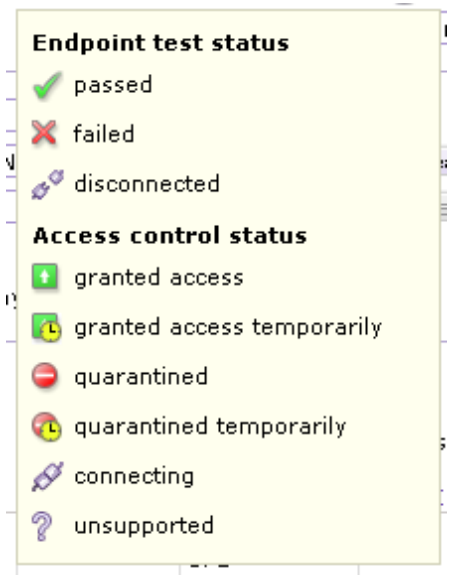


Figure 4-7. Access Control and Endpoint Test Status

NOTE: If an endpoint is seen by two different clusters, the endpoint state can get lost. This could happen, for example, if you had a Training cluster and an Engineering cluster and a laptop that was connected in the Engineering cluster attempted to connect by way of the Training cluster. An error would occur in this case. Make efforts when you are configuring your clusters to avoid this condition.

Selecting Endpoints to Act on

To select endpoint to act on:

NAC 800 Home window>>Endpoint activity

Click a box or boxes in the first column to select the endpoints of interest.

TIP: Click the box at the top of the column to select all of the endpoints.

Acting on Selected Endpoints

Once you have filtered the **Endpoint activity** window and selected which endpoints to take action on, you can perform the following actions:

- Retest an endpoint ("Manually Retest an Endpoint" on page 4-16)
- Allow temporary access for a specific period of time ("Immediately Grant Access to an Endpoint" on page 4-16)
- Temporarily quarantine the endpoint for a specific period of time ("Immediately Quarantine an Endpoint" on page 4-17)
- Clear the temporary quarantine or access state ("Clearing Temporary Endpoint States" on page 4-17)

Manually Retest an Endpoint

To manually retest an endpoint:

NAC 800 Home window>>Endpoint activity

1. Select a box or boxes to select the endpoints of interest.
2. Click **retest**.

Immediately Grant Access to an Endpoint

To immediately grant access to an endpoint:

NAC 800 Home window>>Endpoint activity

1. Select a box or boxes to select the endpoints of interest.
2. Click **change access**.
3. Select the **Temporarily grant access for** radio button.
4. Select **minutes**, **hours**, or **days** from the drop-down list.
5. Enter the number of minutes, hours, or days that the endpoint is allowed access.
6. Click **ok**.

TIP: To quarantine again, select the endpoint, click change access, select Clear temporary access control status, and click ok.

Immediately Quarantine an Endpoint

To immediately quarantine an endpoint:

NAC 800 Home window>>Endpoint activity

1. Select a box or boxes to select the endpoints of interest.
2. Click **change access**.
3. Select the **Temporarily Quarantine for** radio button.
4. Select **minutes**, **hours**, or **days** from the drop-down list.
5. Enter the number of minutes, hours, or days that the endpoint will be temporarily quarantined.
6. Click **ok**.

TIP: To quarantine again, select the endpoint, click change access, select Clear temporary access control status, and click ok.

Clearing Temporary Endpoint States

Endpoints can have a temporary state designated through the **Quarantine for** or **Allow access for** radio buttons. This state is indicated with the words “by admin” in parenthesis in the access states column.

To clear a temporary state set by the admin:

NAC 800 Home window>>Endpoint activity

1. Select a box or boxes to select the endpoints of interest.
2. Click **change access**.
3. Select the **Clear temporary access control status** radio button.
4. Click **ok**.

Viewing Endpoint Information

To view information about an endpoint:

NAC 800 Home window>>Endpoint activity

1. Click on an endpoint name to view the **Endpoint** window:

ProCurve Networking
HP Innovation
Network Access Controller 800
Support | Logout
home > endpoint activity > endpoint (192.168.40.1)
Endpoint
General
Test results
done
Endpoint
NetBIOS: SSD-KGRIFFIN-P3
IP address: 192.168.40.1
MAC address: 00:50:56:C0:00:08
Operating system: Windows XP SP2
Description: unavailable
Access control status: temporarily granted access until May 21, 2007 at 12:48 PM by policy change access
Endpoint test status: fail
802.1X posture: checkup
Testing method: none
Testing NAC policy: Low security
Next test: May 15, 2007 4:48:24 PM MDT
Agentless credentials: (cluster defaults) edit / test credentials
Local user Windows domain: LATIS
Local user ID: unknown
done
© Copyright 2007 Hewlett-Packard Development Company, L.P. 1.0-30216

Figure 4-8. Endpoint, General Option

2. Click **Test results** to view the details of the test:

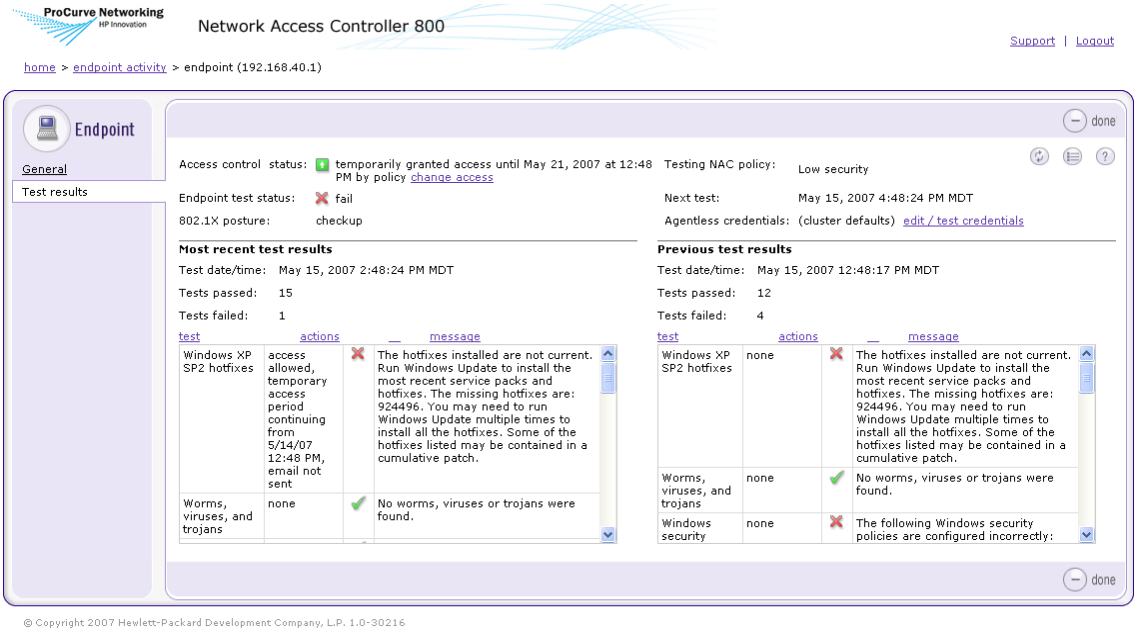

ProCurve Networking
HP Innovation
Network Access Controller 800
Support | Logout
home > endpoint activity > endpoint (192.168.40.1)
Endpoint
General
Test results
done
Access control status: temporarily granted access until May 21, 2007 at 12:48 PM by policy change access
Testing NAC policy: Low security
Endpoint test status: fail
Next test: May 15, 2007 4:48:24 PM MDT
802.1X posture: checkup
Agentless credentials: (cluster defaults) edit / test credentials
Most recent test results
Test date/time: May 15, 2007 2:48:24 PM MDT
Tests passed: 15
Tests failed: 1
test
actions
message
Windows XP SP2 hotfixes
access allowed, temporary access period continuing from 5/14/07 12:48 PM, email not sent
The hotfixes installed are not current. Run Windows Update to install the most recent service packs and hotfixes. The missing hotfixes are: 924496. You may need to run Windows Update multiple times to install all the hotfixes. Some of the hotfixes listed may be contained in a cumulative patch.
Worms, viruses, and trojans
none
No worms, viruses or trojans were found.
Previous test results
Test date/time: May 15, 2007 12:48:17 PM MDT
Tests passed: 12
Tests failed: 4
test
actions
message
Windows XP SP2 hotfixes
none
The hotfixes installed are not current. Run Windows Update to install the most recent service packs and hotfixes. The missing hotfixes are: 924496. You may need to run Windows Update multiple times to install all the hotfixes. Some of the hotfixes listed may be contained in a cumulative patch.
Worms, viruses, and trojans
none
No worms, viruses or trojans were found.
Windows security
none
The following Windows security policies are configured incorrectly:
done
© Copyright 2007 Hewlett-Packard Development Company, L.P. 1.0-30216

Figure 4-9. Endpoint Activity, Endpoint Test Results Option

TIP: Click on any underlined link (for example, change access) to make changes such as changing access or test credentials.

(This page intentionally left blank.)

End-user Access

Chapter Contents

Overview 5-2
Endpoints Supported 5-3
Browser Version 5-4
Browser Settings 5-5
Agentless Settings 5-6
Ports Used for Testing 5-8
Firewall Settings 5-9
- Managed Endpoints 5-9
- Unmanaged Endpoints 5-9
- Allowing the Windows RPC Service Through the Firewall 5-9

End-user Access Windows 5-15
- Opening Window 5-16
- Windows NAC Agent Test Windows 5-17
- ActiveX Test Windows 5-30
- Agentless Test Windows 5-30
- Testing Window 5-33
- Test Successful Window 5-34
- Temporary Quarantine Window 5-35
- Testing Cancelled Window 5-36
- Testing Failed Window 5-37
- Error Windows 5-38

Customizing Error Messages 5-40

Overview

End-users can connect to your network from a number of different types of computers (see “Endpoints Supported” on page 5-3), be tested for compliance based on your definitions in the standard (high, medium, or low security) or custom NAC policies (see “NAC Policies” on page 6-1), and are allowed or denied access based on test results and your quarantine settings (see “Quarantining” on page 3-49). During the login process the end-users are presented with the end-user access windows, which display the testing status and required remediation steps.

This section describes the end-user access windows and options, and details any settings that need to be made on the endpoints.

Endpoints Supported

This NAC 800 release supports the following:

- Windows 98
- Windows 2000
- Windows Server (2000, 2003)
- Windows XP Professional
- Windows XP Home
- Windows NT
- Mac OS (version 10.3.7 or later)

NOTE: Other operating system support (for example Linux) will be included in future releases. Windows ME and Windows 95 are not supported in this release.

TIP: If the end-user switches the Windows view while connected, such as from Classic view to Guest view, the change may not be immediate due to the way sessions are cached.

Browser Version

The browser that should be used is based on the test method as follows:

- ActiveX test method – Microsoft Internet Explorer (IE) version 5.0 or 6.0.
- Agentless and agent-based test methods – IE, Firefox, or Mozilla.

Browser Settings

If the end-user has their IE Internet security zone set to **High**, the endpoint is not testable. Using one of the following options will allow the endpoint to be tested:

- The end-user could change the **Internet security** to **Medium** (**Tools>>Internet options>>Security>>Custom level>>Reset to Medium**).
- The end-user could add the IP address of the NAC 800 server to the **Trusted sites zone**, and then set the **Trusted sites zone** to **Medium.**
- The end-user could customize the **High** setting to allow the options necessary for NAC 800 to test successfully. These options are as follows:
  - The NAC Agent test uses ActiveX
  - The ActiveX test uses ActiveX
  - All of the tests use JavaScript

Agentless Settings

The agentless test method requires file and printer sharing to be enabled.

To enable file and printer sharing on Windows XP Professional:

Endpoint>>Start>>Settings>>Control Panel

1. Double-click **Network connections**.
2. Right-click **Local area connection**.
3. Select **Properties**. The **Local area connection properties** window appears:

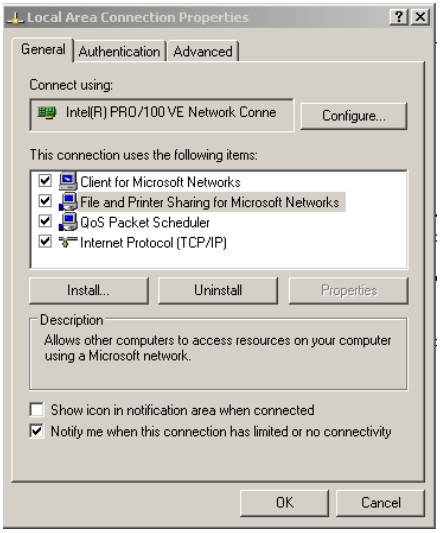


Figure 5-1. Local Area Connection Properties Window

4. On the **General** tab, in the **This connection uses the following** area, verify that **File and Printer sharing** is listed and that the check box is selected.
5. Click **OK**.

For more information on file and printer sharing, refer to the following:

- To configure File and Printer Sharing for Microsoft Networks – http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/howto_config_fileandprintsharing.mspx

- To add a network component – http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/howto_config_fileandprintsharing.mspx

Ports Used for Testing

You might need to configure some firewalls and routers to allow NAC 800 to access the following ports for testing: –

- Agentless test method – 137, 138, 139, and 445
- ActiveX and agent-based test method – 1500

Firewall Settings

NAC 800 can perform tests through firewalls on both managed and unmanaged endpoints.

Managed Endpoints

Typically, a managed endpoint's firewall is controlled with the Domain Group Policy for Windows, or a central policy manager for other firewalls. In this case, the network administrator opens up the agent port or agentless ports only to the NAC 800 server using the centralized policy.

If the Domain Group Policy is not used for Windows endpoints, the appropriate ports are opened during the agent installation process by the NAC 800 installer.

Unmanaged Endpoints

For unmanaged endpoints, the NAC Agent and the ActiveX control test methods automatically open the necessary ports for testing.

End-users connecting with Windows XP, but a non-SP2 firewall (such as Norton) must configure that firewall to allow connection to NAC 800 on port 1500, or the installation of the agent fails.

Allowing the Windows RPC Service Through the Firewall

If end-users enable the XP SP2 Professional firewall, they need to change the configuration to allow the agentless testing.

TIP: These firewall configuration methods can be configured using the Windows Group policy and pushed out to all users of a Windows domain.

The following method is the recommended method:

To configure the Windows XP Professional firewall to allow the RPC service to connect:

Windows>>Start>>Settings>>Control Panel>>Windows Firewall>>Advanced tab>>Settings button

1. Click **Add**.
2. In the **Service Settings** window, enter the following information:

   Description: NAC 800 Server 137
   IP: *<IP of the NAC 800 Server>*
   External port number: 137
   Select **UDP**.
3. Click **OK.**
4. Click **Add**.
5. In the **Service Settings** window, enter the following information:

   Description: NAC 800 Server 138
   IP: *<IP of the NAC 800 Server>*
   External port number: 138
   Select **UDP**.
6. Click **OK.**
7. Click **Add**.
8. In the **Service Settings** window, enter the following information:

   Description: NAC 800 Server 139
   IP: *<IP of the NAC 800 Server>*
   External port number: 139
   Select **TCP**.
9. Click **OK.**
10. Click **Add**.
11. In the **Service Settings** window, enter the following information:

    Description: NAC 800 Server 445
    IP: *<IP of the NAC 800 Server>*
    External port number: 445
    Select **TCP**.
12. Make sure all four rules are selected.
13. Click **OK.**

The following method is an alternate method:

To configure the Windows XP Professional firewall to allow the RPC service to connect:

Windows>>Start>>Settings>>Control Panel>>Windows Firewall>>Exceptions tab

1. Select **File and Print Sharing**. (Verify that the check box is also selected.)
2. Click **Edit**.
3. Verify that the check boxes for all four ports are selected.
4. Select **TCP 139**.
5. Click **Change Scope**.
6. Select **Custom List.**
7. Enter the NAC 800 Server IP address and the `255.255.255.0` mask.
8. Click **OK**.
9. Select **UDP 137**.
10. Click **Change Scope**.
11. Select **Custom List.**
12. Enter the NAC 800 Server IP address and the `255.255.255.0` mask.
13. Click **OK**.
14. Select **TCP 445**.
15. Click **Change Scope**.
16. Verify that the **My network (subnet) only** radio button is selected.
17. Click **OK.**
18. Select **UDP 138**.
19. Click **Change Scope**.
20. Verify that the **My network (subnet) only** radio button is selected.
21. Click **OK.**
22. Click **OK.**
23. Click **OK.**

TIP: You can add more security by specifying the endpoints allowed for File and Print Sharing as follows:

Select File and Print Sharing, Click Edit, Select Change Scope, and select either My Network or Custom List (and then specify the endpoints).

Allowing NAC 800 through the OS X Firewall

To verify that NAC 800 can test the end-user through the end-user's firewall:

Apple Menu>>System Preferences

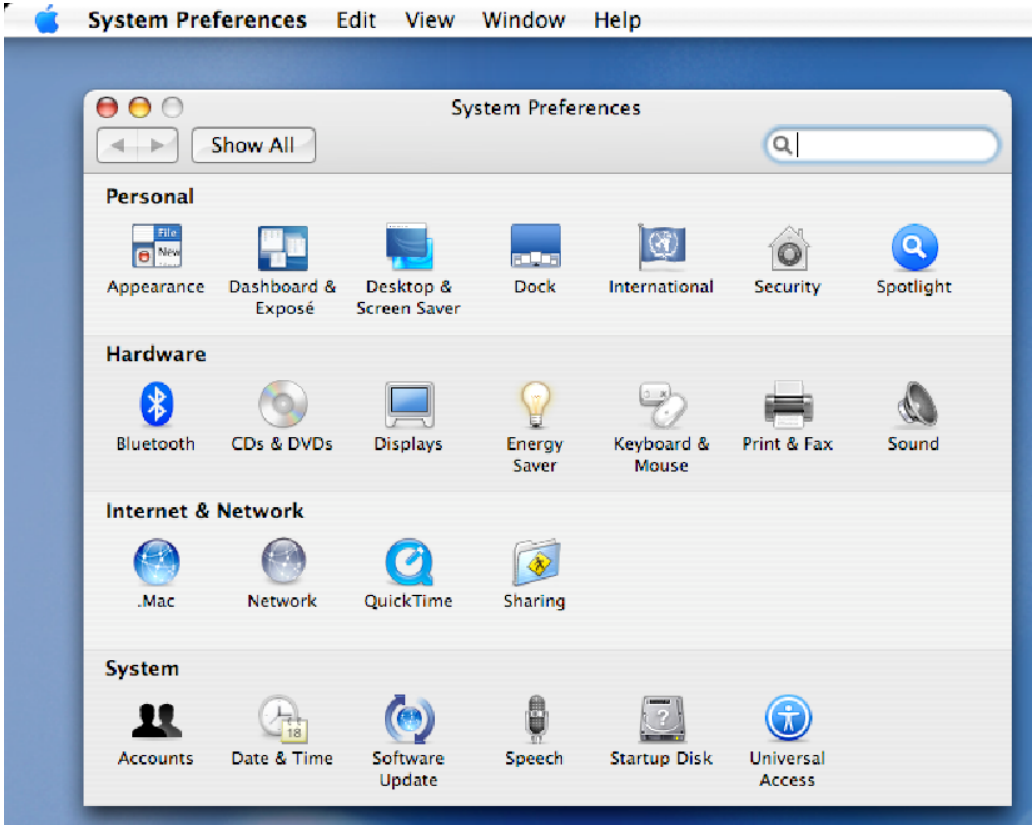


Figure 5-2. Mac System Preferences Window

1. Select the **Sharing** icon. The **Sharing** window opens.

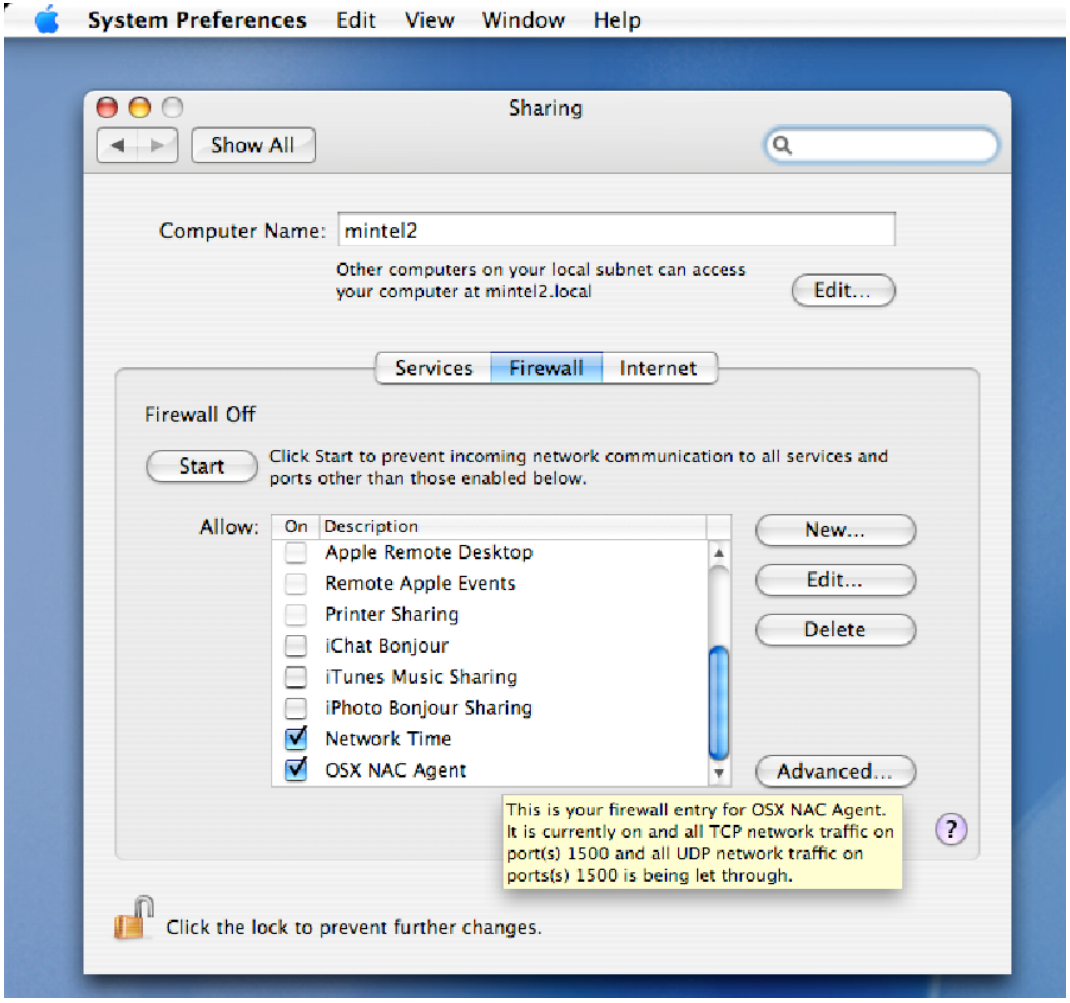


Figure 5-3. Mac Sharing Window

2. Select the **Firewall** tab.
3. The firewall settings must be one of the following:
   - Off
   - On with the following:
     – OS X NAC Agent check box selected
     – Port 1500 open

To change the port:

Apple Menu>>System Preferences>>Sharing icon>>Firewall tab

1. Select OS X NAC Agent.
2. Click Edit. The port configuration window appears:

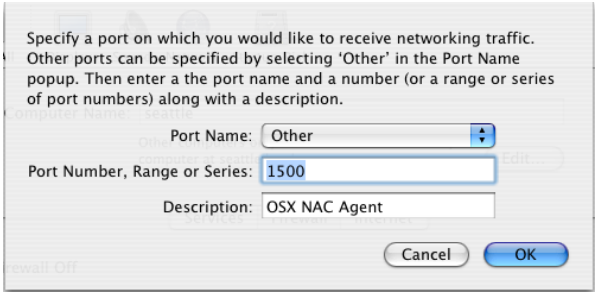

Specify a port on which you would like to receive networking traffic. Other ports can be specified by selecting 'Other' in the Port Name popup. Then enter a the port name and a number (or a range or series of port numbers) along with a description.
Port Name:
Other
Port Number, Range or Series:
1500
Description:
OSX NAC Agent
Cancel
OK

Figure 5-4. Mac Ports Window

3. Enter `1500` in the **Port Number, Range or Series** text field.
4. Click **OK**.

End-user Access Windows

Several end-user access templates come with NAC 800. The **End-user** window provides a way to customize these templates from within the console (see "End-user Screens" on page 3-104). For optimal end-user experience, brand these windows as your own and keep them friendly and helpful. It is important to convey to your end-users what is happening during and after the testing process.

If you want to make more customizations than are available using the **End-user** window, the files are located in the following directory:

```
/usr/local/nac/webapps/HoldingArea
```

There are two ways you can edit the NAC 800 end-user access templates outside of the ProCurve console configuration window:

- UNIX command line and vi text editor – Connect to the NAC 800 server using SSH, then edit the files with `vi`.
- HTML editor on your local machine – Connect to the NAC 800 server using SSH, copy the files to your local machine, edit the files with any HTML or text editor, copy the files back to the NAC 800 server.

You can also create additional HTML files.

NOTE: Upgrading the NAC 800 software does not overwrite your template changes. Your updated templates are preserved.

CAUTION: Do not rename the files or they will not be seen by NAC 800.

End-users begin the login process by opening their browser. If their home page is defined on the **Accessible services** window, they are allowed to access that page.

Opening Window

When the end-user directs their browser to go to a location that is not listed in the **Accessible services and endpoints** list, the testing option window appears:

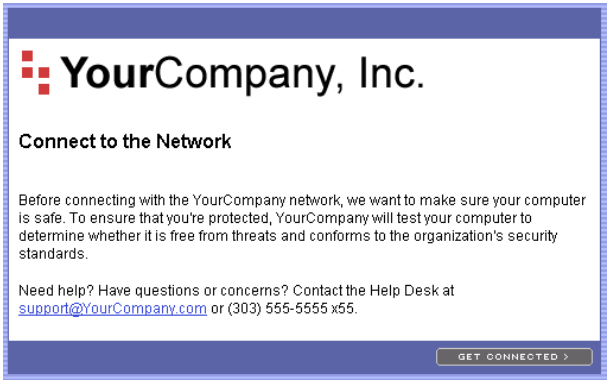

YourCompany, Inc.
Connect to the Network
Before connecting with the YourCompany network, we want to make sure your computer is safe. To ensure that you're protected, YourCompany will test your computer to determine whether it is free from threats and conforms to the organization's security standards.
Need help? Have questions or concerns? Contact the Help Desk at support@YourCompany.com or (303) 555-5555 x55.
GET CONNECTED >

Figure 5-5. End-user Opening Window

The end-users select **Get connected**. One of the following windows appears, depending on which test method and order is specified in the **System configuration>>Testing methods** window:

- Windows NAC Agent test – Installation window (first-time connection only) (see “Windows NAC Agent Test Windows” on page 5-17)
- ActiveX test – Testing window (see “ActiveX Test Windows” on page 5-30)
- Agentless test – Testing window (see “Agentless Test Windows” on page 5-30)

If the **Allow end users to cancel installation** option on the **System Configuration>>Testing methods** window is selected, the end-users have the option of clicking **Cancel installation**. If they click **Cancel installation**, an **Installation cancelled** window appears.

TIP: The logo and the text in figure 5-5 is customizable as described in “End-user Screens” on page 3-104.

Windows NAC Agent Test Windows

Automatically Installing the Windows Agent

When the test method used is **NAC Agent test**, the first time the user attempts to connect, the agent installation process should begin automatically, and the installing window appears:

YourCompany, Inc.
Software is being installed for testing your computer.
Please wait...
If the installation is not complete in 30 seconds, please click here.
CANCEL INSTALLATION

Figure 5-6. End-user Installing Window

TIP: The end-user can also manually install the agent as described in “Manually Installing the Windows Agent” on page 5-20.

If Active Content is disabled in the browser, the following error window appears:

YourCompany, Inc.
Testing software installation failed
Installation of the testing software failed.
Did you see an information bar like?
Back
Address
https://10.0.20.15:89/index.jsp?action_type=
The previous site might require the following ActiveX cont
If so, click on it and select Install ActiveX Control.
More suggestions
Download the software manually
To download and install the software yourself, do the following:
1. Download the testing software.
2. Run the software, following the step-by-step instructions.
3. Click begin testing to have your computer tested.
For assistance, call the Help Desk at (303) 555-5555 or email support@company.com.
Diagnostics
TRY INSTALLATION AGAIN

Figure 5-7. End-user Agent Installation Failed

TIP: To enable active content, see “Active Content” on page B-3.

If this is the first time the end-user has selected **NAC Agent test**, a security acceptance window appears. In order to proceed with the test, the user must select to **Install** the digital signature.

Once the user has accepted the digital signature, the agent installation begins. The user must click Next to start the agent installation:

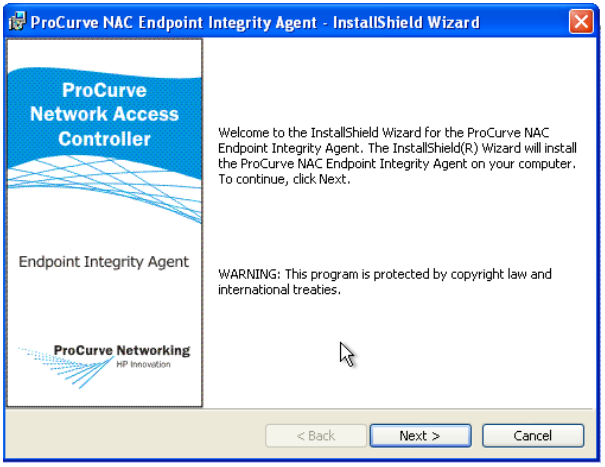

ProCurve NAC Endpoint Integrity Agent - InstallShield Wizard
ProCurve Network Access Controller
Endpoint Integrity Agent
ProCurve Networking
HP Innovation
Welcome to the InstallShield Wizard for the ProCurve NAC Endpoint Integrity Agent. The InstallShield(R) Wizard will install the ProCurve NAC Endpoint Integrity Agent on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

Figure 5-8. End-user Agent Installation Window (Start)

The user must click **Finish** to complete the agent installation and begin testing:

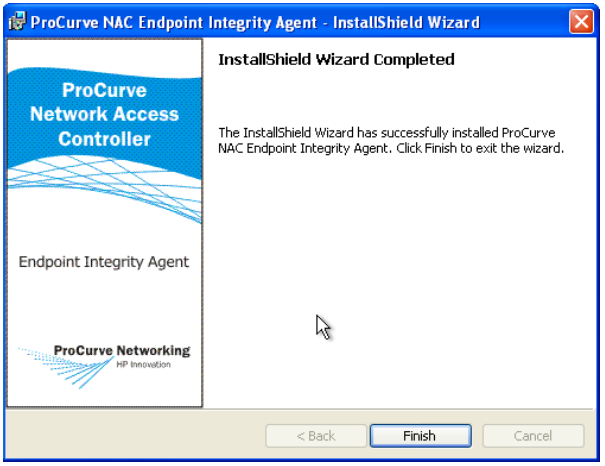

ProCurve NAC Endpoint Integrity Agent - InstallShield Wizard
ProCurve Network Access Controller
Endpoint Integrity Agent
ProCurve Networking
HP Innovation
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed ProCurve NAC Endpoint Integrity Agent. Click Finish to exit the wizard.
< Back
Finish
Cancel

Figure 5-9. End-user Agent Installation Window (Finish)

As soon as the installation is complete, the endpoint is tested. See “Testing Window” on page 5-33.

Removing the Agent

To remove the agent:

Start button>>Settings>>Control panel>>Add/remove programs

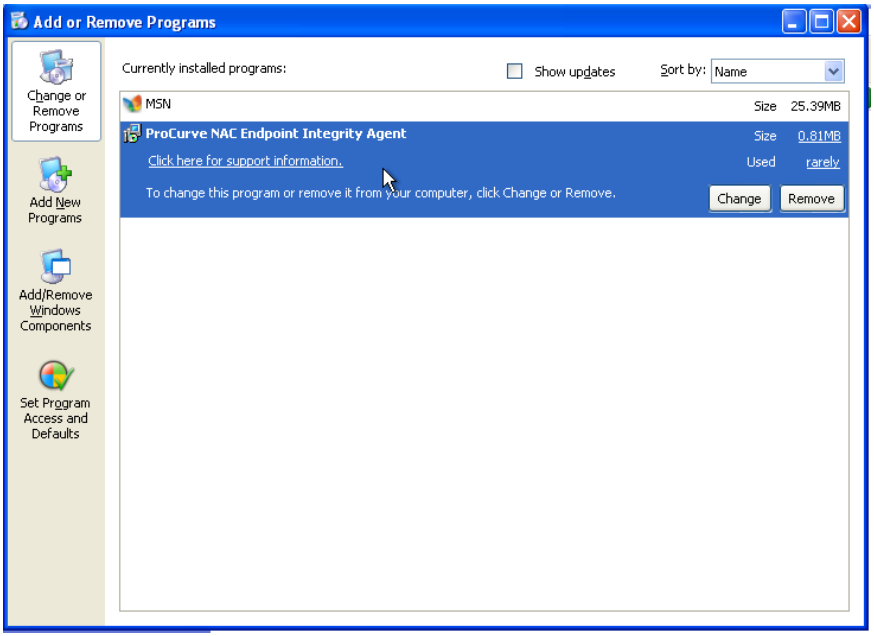


Figure 5-10. Add/Remove Programs

1. Find the **ProCurve NAC EI Agent** in the list of installed programs.
2. Click **Remove**.

TIP: The ProCurve NAC EI Agent also appears in the services list:

Start button>>Settings>>Control panel>>Administrative tools>>Services

Manually Installing the Windows Agent

To manually install the agent (using Internet Explorer):

Endpoint>>IE browser window

1. Point the browser to the following URL:

   `https://<enforcement_server_ip>:89/setup.exe`

   The security certificate window appears:

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

Figure 5-11. Security Certificate Window

2. Click **Yes** to accept the security certificate. You are prompted to select **Save** to disk or **Run** the file:

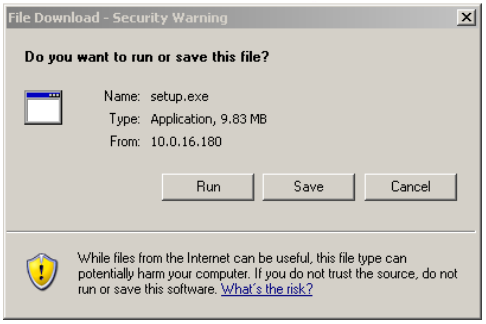

File Download - Security Warning
Do you want to run or save this file?
Name: setup.exe
Type: Application, 9.83 MB
From: 10.0.16.180
Run
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Figure 5-12. Run or Save to Disk Window

3. Click **Run** to begin the install process.
4. The Agent Installation Wizard starts (Figure 5-8 on page 5-19).

How to View the Windows Agent Version Installed

To see what version of the agent the endpoint is running:

Command line window on the endpoint

1. Change the working directory to the following:

   ```
   C:\Program Files\Hewlett-Packard\ProCurve NAC
   Endpoint Integrity Agent
   ```

2. Enter the following command:

   ```
   SAService version
   ```

   The version number is returned. For example: `4,0,0,567`

Mac OS Agent Test Windows

When the test method selected is agent-based, the first time the end-user logs in to their Macintosh computer and opens a browser window, NAC 800 attempts to test the endpoint. If the agent is required, they receive the Installation Failed window shown in figure 5-7.

Installing the MAC OS Agent

To install the Mac OS agent:

The Mac OS agent must be installed manually and works with Mac OS X version 10.3.7 or later. Both the PowerPC and Intel Macintosh computers are supported. To check your version of Mac OS, select **Apple Menu>>About This Mac**.

1. Click the **download** the testing software link (figure 5-7).
2. Double-click the downloaded file to unzip it.
3. Double-click the extracted file to launch the installer program. A confirmation window appears:

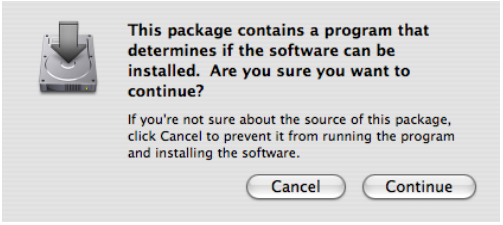

This package contains a program that determines if the software can be installed. Are you sure you want to continue?
If you're not sure about the source of this package, click Cancel to prevent it from running the program and installing the software.
Cancel
Continue

Figure 5-13. Start Mac OS Installer Window

4. Click **Continue**. The installer appears:

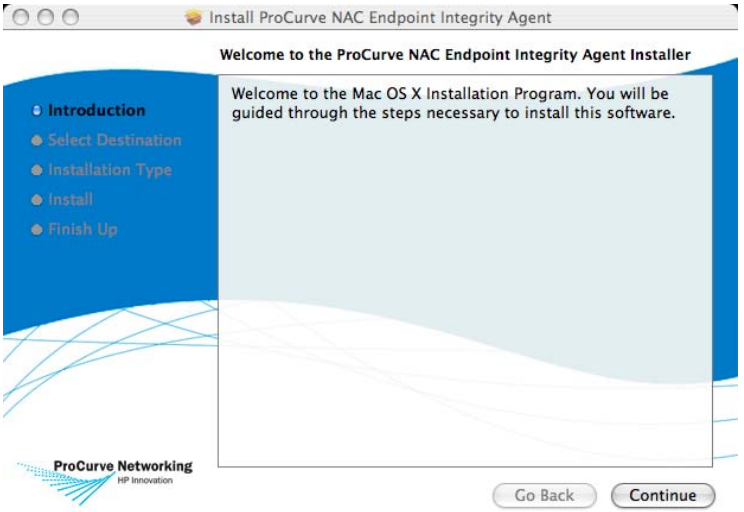

Install ProCurve NAC Endpoint Integrity Agent
Welcome to the ProCurve NAC Endpoint Integrity Agent Installer
Introduction
Select Destination
Installation Type
Install
Finish Up
Welcome to the Mac OS X Installation Program. You will be guided through the steps necessary to install this software.
ProCurve Networking
HP Innovation
Go Back
Continue

Figure 5-14. Mac OS Installer Window 1 of 5

5. Click **Continue**. The **Select a Destination** window appears:

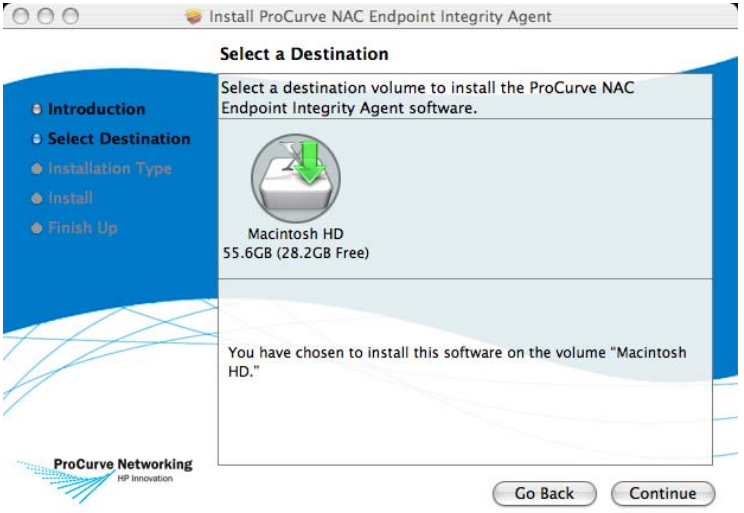


Figure 5-15. Mac OS Installer Window 2 of 5

6. Click **Continue**. The **Easy Install** window appears:

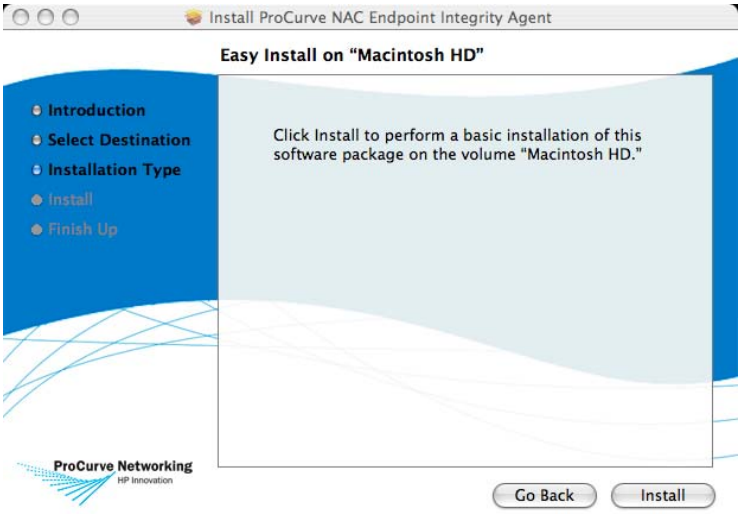


Figure 5-16. Mac OS Installer Window 3 of 5

7. Click **Install**. The **Authenticate** window appears:

Figure 5-17. Mac OS Installer Window 4 of 5

8. Enter your password. Click **OK**. The agent is installed and the confirmation window appears:

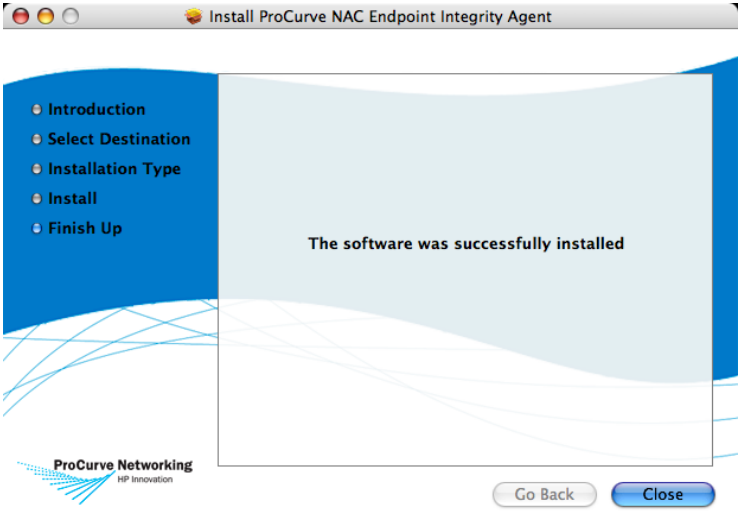


Figure 5-18. Mac OS Installer Window 5 of 5

9. Click **Close**.

Verifying the Mac OS Agent

To verify that the Mac OS agent is running properly:

Double-click Desktop icon>>Aplication folder>>Utilities folder

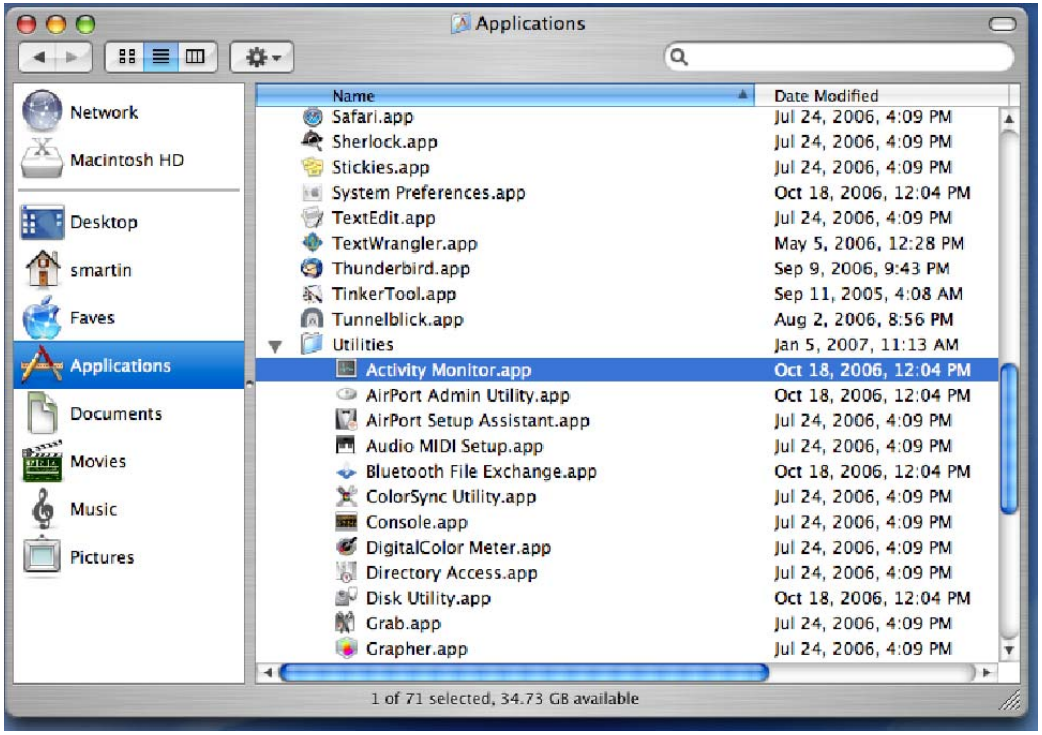


Figure 5-19. Applications Window, Utilities Folder

1. Double-click Activity Monitor. The Activity Monitor window appears:

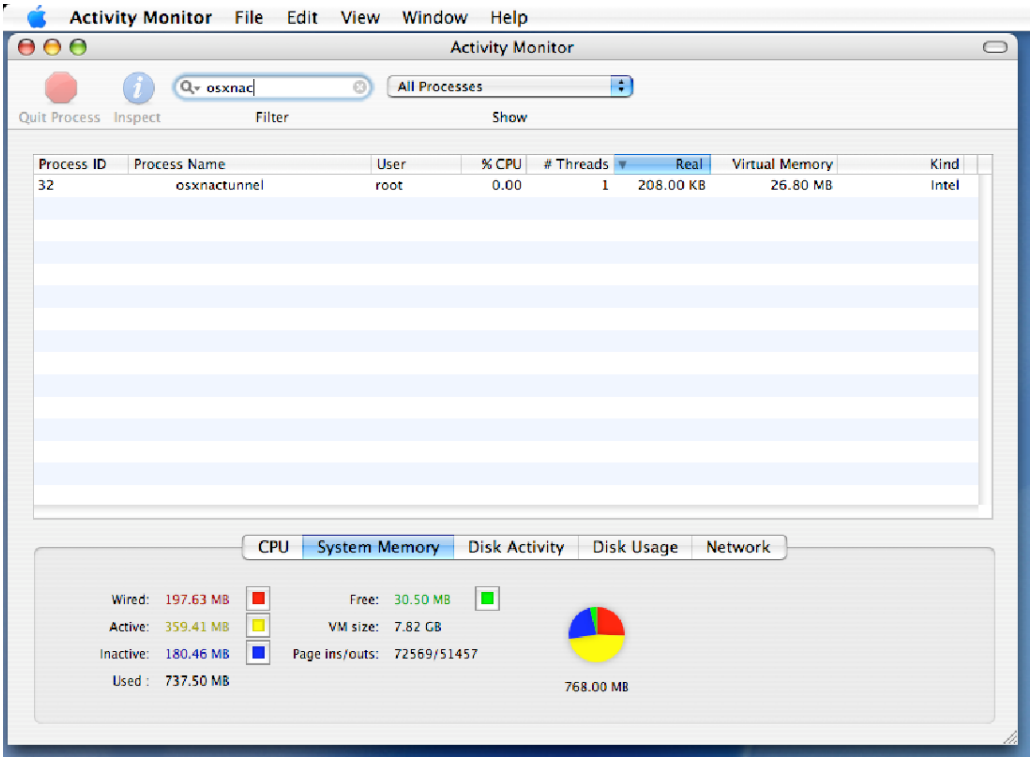


Figure 5-20. Activity Monitor Window

2. Verify that the **osxnactunnel** process is running.
3. If the **osxnactunnel** process is not running, start it by performing the following steps:

a. Select **Applications window>>Utilities>>Mac OS X Terminal**. A terminal window opens:

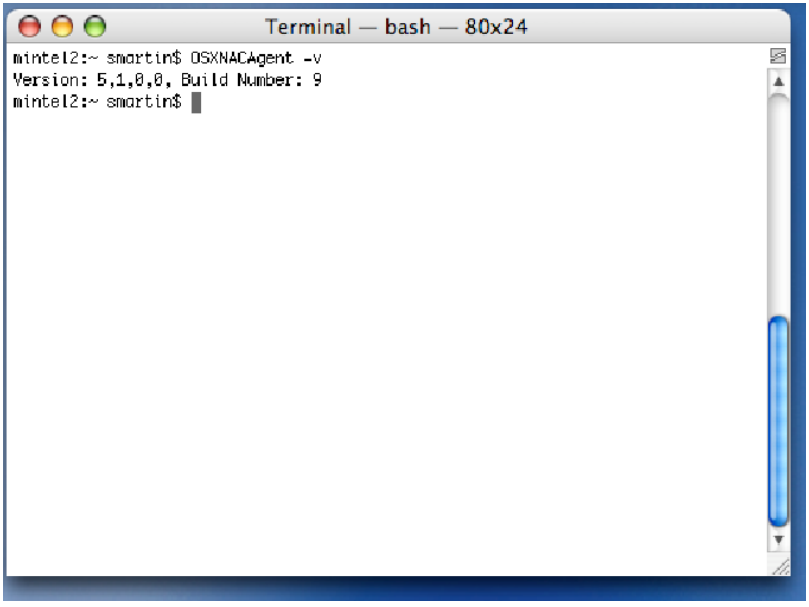


Figure 5-21. Mac Terminal Window

b. Enter the following at the command line:

```
OSXNACAgent -v
```

The build and version number are returned.

c. If an error message is returned indicating that the agent could not be found, the agent was not installed properly. Re-install the agent as described in “Installing the MAC OS Agent” on page 5-22.

d. If the agent is installed but not running, enter the following at the command line:

```
sudo OSXNACAgentDaemon restart
```

e. Check the **Activity Monitor** window again to see if the **osxnactunnel** process is running. If it is still not functioning properly after re-installing the agent and attempting to restart the process, contact your network administrator for assistance.

Removing the Mac OS Agent

To remove the Mac OS agent:

Double-click Desktop icon>>Aplication folder>>Utilities folder

1. Select **Mac OS X Terminal**. A terminal window opens (figure 5-21).
2. Enter the following at the command line:

   ```
   remove_osxnacagent
   ```

3. Remove the firewall entry:
   a. Select **Apple Menu>>System Preferences>>Sharing->Firewall** tab.
   b. Select **OS X NAC Agent**.
   c. Click **Delete**.

ActiveX Test Windows

For the **ActiveX test**, the **Testing** window appears (see “Testing Window” on page 5-33) and an ActiveX component is downloaded. If there is an error running the ActiveX component, an error window appears:

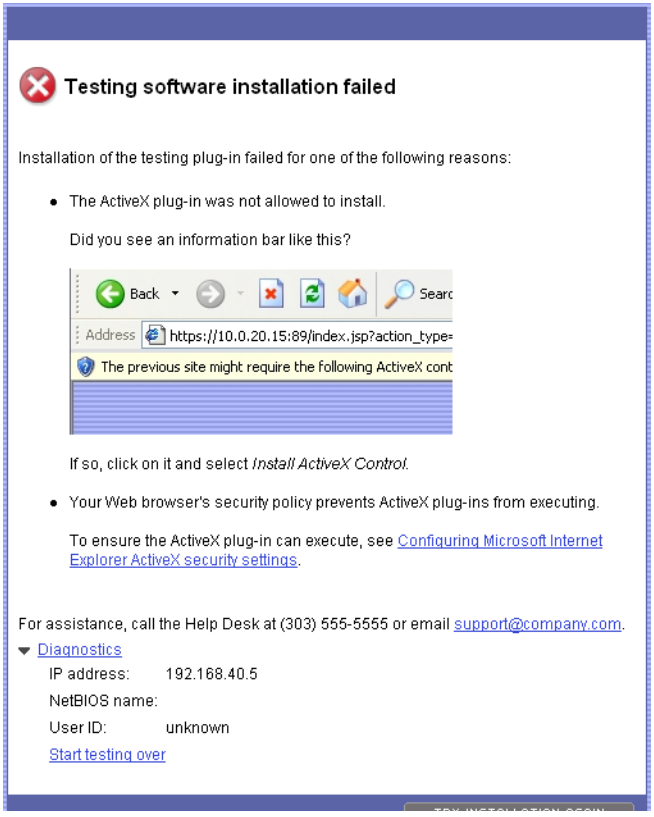

Testing software installation failed
Installation of the testing plug-in failed for one of the following reasons:
The ActiveX plug-in was not allowed to install.
Did you see an information bar like this?
Back
Address
https://10.0.20.15:89/index.jsp?action_type=
The previous site might require the following ActiveX cont
If so, click on it and select Install ActiveX Control.
Your Web browser's security policy prevents ActiveX plug-ins from executing.
To ensure the ActiveX plug-in can execute, see Configuring Microsoft Internet Explorer ActiveX security settings.
For assistance, call the Help Desk at (303) 555-5555 or email support@company.com.
Diagnostics
IP address: 192.168.40.5
NetBIOS name:
User ID: unknown
Start testing over

Figure 5-22. End-user ActiveX Plug-in Failed Window

TIP: To enable active content, see “Active Content” on page B-3.

Agentless Test Windows

If the end-users select **Agentless test**, NAC 800 needs login credentials in order to test the endpoint. Credentials can be obtained from the following:

- Automatically connect the user through domain authentication (“Agentless Credentials” on page 3-107)

- Require the user to log in. End-users must set up their local endpoints to have a Windows administrator account with a password in order to be tested by NAC 800.

NOTE: NAC 800 uses the Windows Messenger Service when using agentless testing. If you have disabled this service (http://www.microsoft.com/windowsxp/using/security/learnmore/stopspam.mspx), agentless testing will not work.

TIP: If the end-user has not defined a login/password combination, the default login is usually `administrator` with a blank password.

If the end-users are required to log in, or if the automatic connection methods fail, they must log in using the following window:

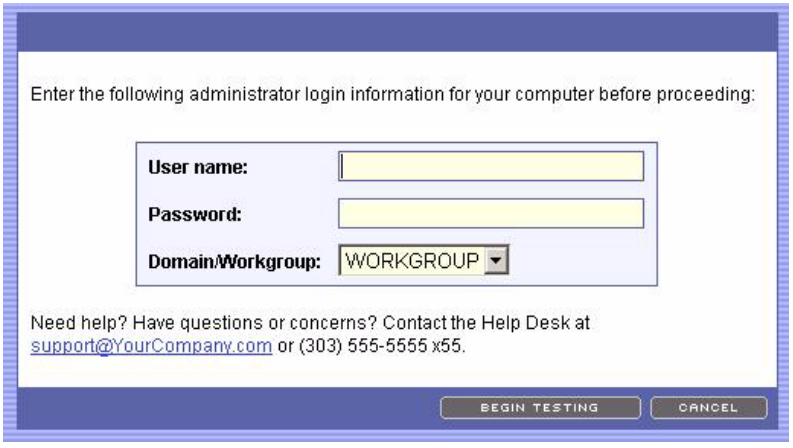


Figure 5-23. End-user Login Credentials Window

If the **Allow end-users to have their administrator login information saved for future access** option is selected on the **System Configuration>>Testing methods** window, the end-user login window presents a check box option to the end-users, allowing them to save their login credentials.

If the login credentials are correct, the **Testing** window is displayed (see "Testing Window" on page 5-33).

If the end-users do not enter the correct information in the login window fields, a login failure window appears:

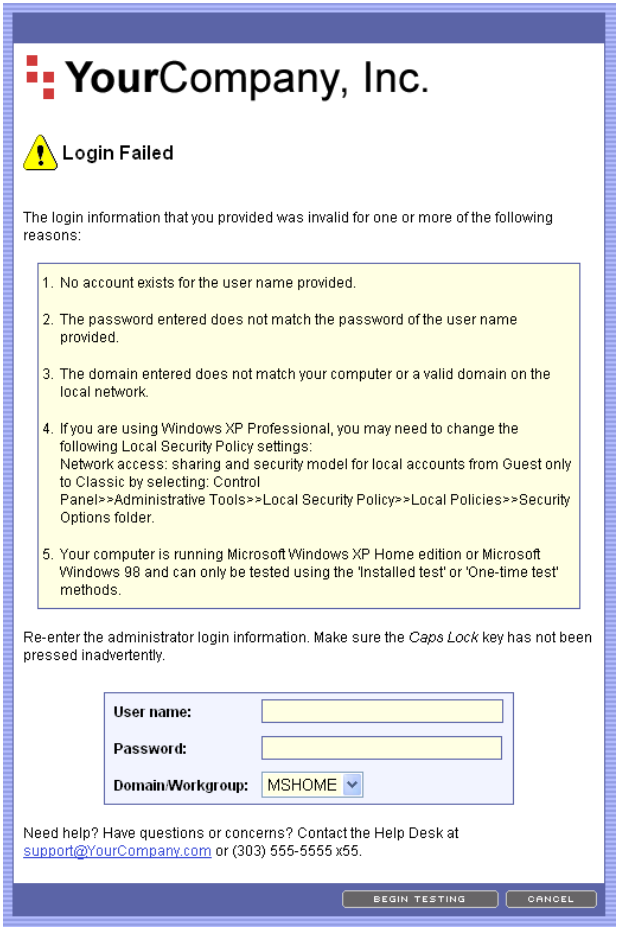

YourCompany, Inc.
Login Failed
The login information that you provided was invalid for one or more of the following reasons:
1. No account exists for the user name provided.
2. The password entered does not match the password of the user name provided.
3. The domain entered does not match your computer or a valid domain on the local network.
4. If you are using Windows XP Professional, you may need to change the following Local Security Policy settings:
Network access: sharing and security model for local accounts from Guest only to Classic by selecting: Control Panel>>Administrative Tools>>Local Security Policy>>Local Policies>>Security Options folder.
5. Your computer is running Microsoft Windows XP Home edition or Microsoft Windows 98 and can only be tested using the 'Installed test' or 'One-time test' methods.
Re-enter the administrator login information. Make sure the Caps Lock key has not been pressed inadvertently.
User name:
Password:
Domain/Workgroup:
MSHOME
Need help? Have questions or concerns? Contact the Help Desk at support@YourCompany.com or (303) 555-5555 x55.
BEGIN TESTING
CANCEL

Figure 5-24. End-user Login Failed

TIP: You can customize the logo and contact paragraph that appear on this window. See “Customizing Error Messages” on page 5-40 for more details.

Testing Window

The following figure shows the window that appears during the testing process:

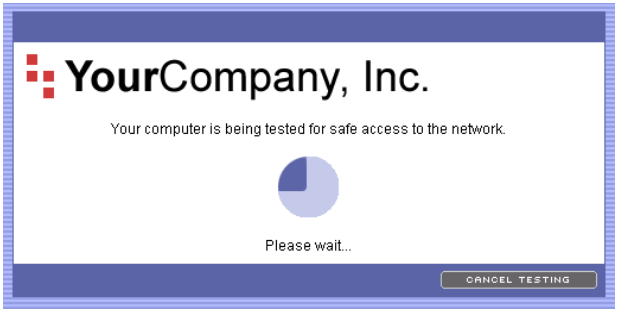


Figure 5-25. End-user Testing Window

The possible outcomes from the test are as follows:

- Test successful window (see “Test Successful Window” on page 5-34)
- Temporary quarantine window (see “Temporary Quarantine Window” on page 5-35)
- Testing cancelled window (see “Testing Cancelled Window” on page 5-36)
- Testing failed window (see “Testing Failed Window” on page 5-37)
- Other error window (see “Error Windows” on page 5-38)

Test Successful Window

When the end-users' endpoints meet the test criteria defined in the NAC policy, they are allowed access to the network, and a window indicating successful testing appears:

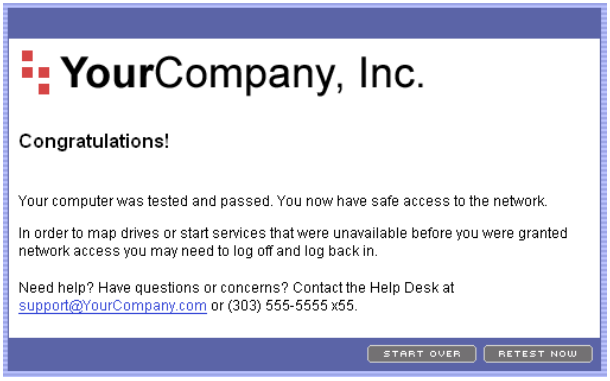

YourCompany, Inc.
Congratulations!
Your computer was tested and passed. You now have safe access to the network.
In order to map drives or start services that were unavailable before you were granted network access you may need to log off and log back in.
Need help? Have questions or concerns? Contact the Help Desk at support@YourCompany.com or (303) 555-5555 x55.
START OVER
RETEST NOW

Figure 5-26. End-user Testing Successful Window

TIP: You can customize the logo and text that appears on this window as described in "End-user Screens" on page 3-104.

Temporary Quarantine Window

When the end-users meet the test criteria defined in the NAC policy, but the NAC 800 **Quarantine all** setting is enabled, the quarantine window appears:

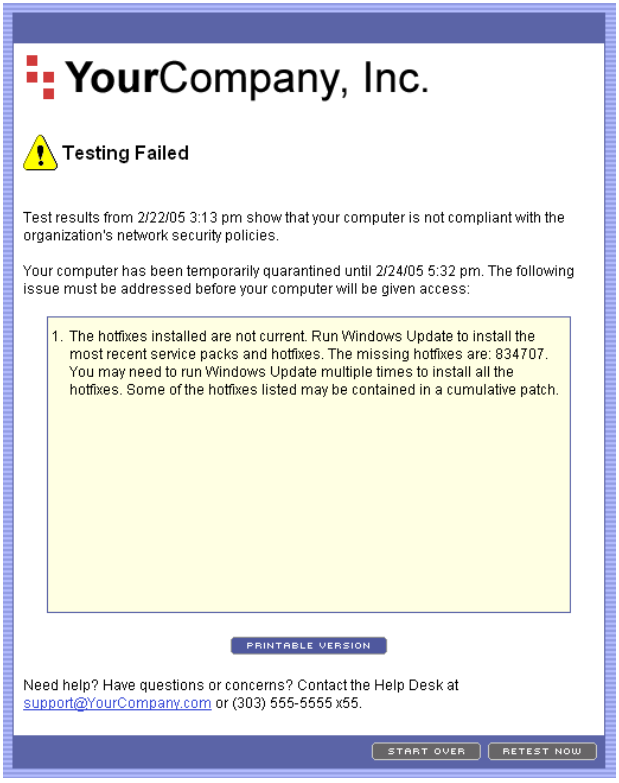

YourCompany, Inc.
Testing Failed
Test results from 2/22/05 3:13 pm show that your computer is not compliant with the organization's network security policies.
Your computer has been temporarily quarantined until 2/24/05 5:32 pm. The following issue must be addressed before your computer will be given access:
1. The hotfixes installed are not current. Run Windows Update to install the most recent service packs and hotfixes. The missing hotfixes are: 834707. You may need to run Windows Update multiple times to install all the hotfixes. Some of the hotfixes listed may be contained in a cumulative patch.
PRINTABLE VERSION
Need help? Have questions or concerns? Contact the Help Desk at support@YourCompany.com or (303) 555-5555 x55.
START OVER
RETEST NOW

Figure 5-27. Temporary Quarantine Window

TIP: You can customize the logo and contact paragraph that appear on this window. See “Customizing Error Messages” on page 5-40 for more details.

Testing Cancelled Window

If the **Allow end users to cancel testing** option on the **System configuration>>Testing methods** window is selected, the end-user has the option of clicking **Cancel testing**. If the end-users click **Cancel testing**, a window appears indicating that testing is cancelled:

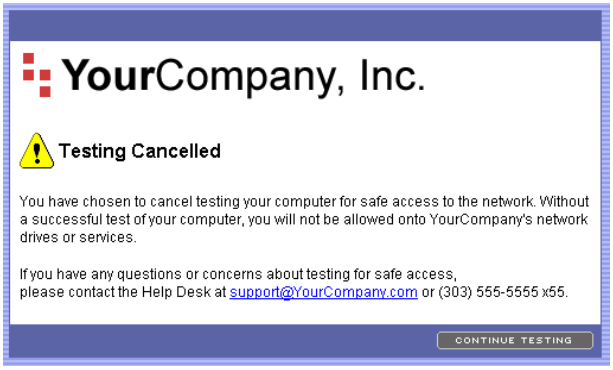

YourCompany, Inc.
Testing Cancelled
You have chosen to cancel testing your computer for safe access to the network. Without a successful test of your computer, you will not be allowed onto YourCompany's network drives or services.
If you have any questions or concerns about testing for safe access, please contact the Help Desk at support@YourCompany.com or (303) 555-5555 x55.
CONTINUE TESTING

Figure 5-28. End-user Testing Cancelled Window

Testing Failed Window

When the end-user's endpoints fail to meet the test criteria defined in the NAC policy, the end-users are not allowed access to the network (are quarantined) and the following testing failed window appears:

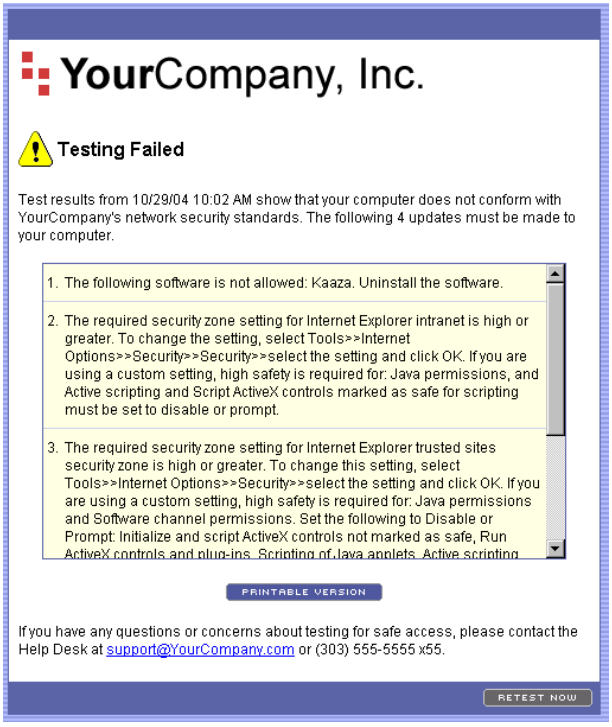

YourCompany, Inc.
Testing Failed
Test results from 10/29/04 10:02 AM show that your computer does not conform with YourCompany's network security standards. The following 4 updates must be made to your computer.
1. The following software is not allowed: Kaaza. Uninstall the software.
2. The required security zone setting for Internet Explorer intranet is high or greater. To change the setting, select Tools>>Internet Options>>Security>>Security>>select the setting and click OK. If you are using a custom setting, high safety is required for: Java permissions, and Active scripting and Script ActiveX controls marked as safe for scripting must be set to disable or prompt.
3. The required security zone setting for Internet Explorer trusted sites security zone is high or greater. To change this setting, select Tools>>Internet Options>>Security>>select the setting and click OK. If you are using a custom setting, high safety is required for: Java permissions and Software channel permissions. Set the following to Disable or Prompt: Initialize and script ActiveX controls not marked as safe, Run ActiveX controls and plug-ins, Scripting of Java applets, Active scripting
PRINTABLE VERSION
If you have any questions or concerns about testing for safe access, please contact the Help Desk at support@YourCompany.com or (303) 555-5555 x55.
RETEST NOW

Figure 5-29. End-user Testing Failed Window Example 1

TIP: You can elect to allow access to specific services and endpoints by including them in the Accessible services and endpoints area of the System configuration>>Accessible services window (see "Accessible Services" on page 3-98).

TIP: You can customize the logo and contact paragraph that appear on this window. See "Customizing Error Messages" on page 5-40 for more details.

End-users can click **Printable version** to view the testing results in a printable format, as shown in the following figure:

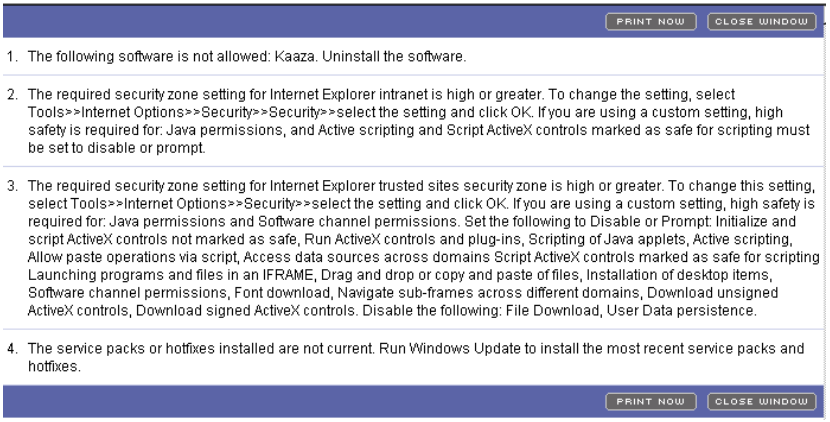

PRINT NOW
CLOSE WINDOW
1. The following software is not allowed: Kaaza. Uninstall the software.
2. The required security zone setting for Internet Explorer intranet is high or greater. To change the setting, select Tools>>Internet Options>>Security>>Security>>select the setting and click OK. If you are using a custom setting, high safety is required for: Java permissions, and Active scripting and Script ActiveX controls marked as safe for scripting must be set to disable or prompt.
3. The required security zone setting for Internet Explorer trusted sites security zone is high or greater. To change this setting, select Tools>>Internet Options>>Security>>select the setting and click OK. If you are using a custom setting, high safety is required for: Java permissions and Software channel permissions. Set the following to Disable or Prompt: Initialize and script ActiveX controls not marked as safe, Run ActiveX controls and plug-ins, Scripting of Java applets, Active scripting, Allow paste operations via script, Access data sources across domains Script ActiveX controls marked as safe for scripting Launching programs and files in an IFRAME, Drag and drop or copy and paste of files, Installation of desktop items, Software channel permissions, Font download, Navigate sub-frames across different domains, Download unsigned ActiveX controls, Download signed ActiveX controls. Disable the following: File Download, User Data persistence.
4. The service packs or hotfixes installed are not current. Run Windows Update to install the most recent service packs and hotfixes.
PRINT NOW
CLOSE WINDOW

Figure 5-30. End-user Testing Failed, Printable Results Window

Setting the Temporary Access Period

For each NAC policy, you can specify a temporary access period should the end-users fail the tests.

To set the temporary access period:

NAC 800 Home window>>NAC policies>>NAC policy of interest>>Tests menu option>>Select a test failure action

1. Select from the following:
   - **Send an email notification to the NAC 800 administrator**
   - **Quarantine access**
     - **Immediately**
     - **Grant temporary access for ___ days** and enter a number in the text box. A message appears on the **Access approved** window informing the users that they have temporary access to bring their system into compliance.
2. Click **OK**.

Error Windows

End-users might see any of the following error windows:

- Unsupported endpoint
- Unknown error

The following figure shows an example of an error window:

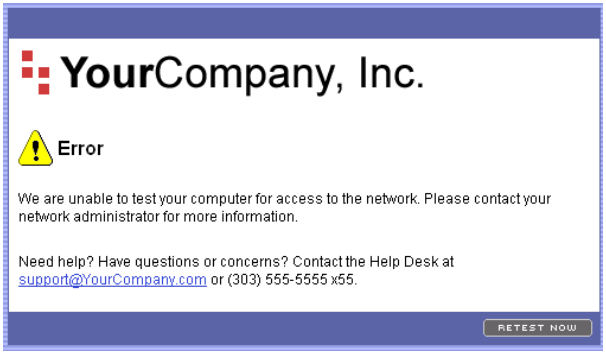

YourCompany, Inc.
Error
We are unable to test your computer for access to the network. Please contact your network administrator for more information.
Need help? Have questions or concerns? Contact the Help Desk at support@YourCompany.com or (303) 555-5555 x55.
RETEST NOW

Figure 5-31. End-user Error Window

Customizing Error Messages

The default error message strings (remediation messages) are defined in the following file:

```
/usr/local/nac/scripts/BaseClasses/Strings.py
```

You can create custom error message strings that appear in the test result reports, and on the test results access window that the end-user views by editing or creating the following file:

```
/usr/local/nac/scripts/BaseClasses/CustomStrings.py
```

To customize the error messages:

1. Create a file using a text editor, and name it as follows:

   ```
   /usr/local/nac/scripts/BaseClasses/CustomStrings.py
   ```

   using the following format:

   ```
   class CustomStrings:

             stringTable = {
                "name1" : "message1",
                "name2" : "message2",
               }
   ```

   Where:

   The name value (`name1`) matches the name of the test (see table 5-1 on page 541).

   The message value (`message1`) is the text you want to appear in the reports and on the end-user access windows.

   For example:

   ```
   class CustomStrings:

           stringTable = {
             "checkAntiVirusUpdates.String.1" : "The
   required anti-virus software was not found.  Install
   ```

```
the software from this location <a href='http://
myserver.someplace.com/dir/application.exe'>Location
Name</a>",
          "name2" : "message2",
        }
```

NOTE: A "%s" in the description text is a special variable that is interpolated into extra information (passed from NAC 800) such as lists of missing patches, or missing software.

NOTE: While editing the description avoid the use of double quotes "". Use single quotes instead. Double quotes will get interpreted by the software and can cut the string short or cause the replacement to fail.

2. Restart the `nac` process by entering the following command:

```
service nac restart
```

Test name	Description
checkAntiVirusUpdates.String.1	The required anti-virus software was not found. Install anti-virus software and keep the virus definitions up-to-date. Supported Anti Virus software: %s,
checkAntiVirusUpdates.String.2	%s is installed but the service is not running and the virus signatures are not up-to-date (installed: %s required: %s).,
checkAntiVirusUpdates.String.3	%s is installed but the service is not running.,
checkAntiVirusUpdates.String.4	(version: %s),
checkAntiVirusUpdates.String.5	%s is installed but the virus signatures are not up-to-date (installed: %s required: %s).,
checkAntiVirusUpdates.String.6	The %s service is running and virus signatures are up-to-date.,
checkAutoUpdateStatus.String.1	The OS is not relevant to this test.,
checkAutoUpdateStatus.String.2	The auto_update_level_required parameter is required.,

Table 5-1.Default Test Names and Descriptions

Test name	Description
checkAutoUpdateStatus.String.3	Automatic Updates have not been configured. For Windows 2000, install Service Pack 4, then enable Automatic Updates by selecting: Control Panel>>Automatic Updates. For Windows XP: select Control Panel>>System>>Automatic Updates tab.,
checkAutoUpdateStatus.String.4	Automatic Updates are set to: %s,
checkAutoUpdateStatus.String.5	Automatic Updates must be configured to %s. For Windows 2000, install Service Pack 4, then enable Automatic Updates by selecting: Control Panel>>Automatic Updates. For Windows XP: select Control Panel>>System>>Automatic Updates tab.,
checkAutoUpdateStatus.String.6	The Automatic Update client has been disabled. Ask your local System Administrator for instructions on how to enable it.,
checkHotFixes.String.1	An unsupported operating system was encountered.,
checkHotFixes.String.2	The OS is not relevant to this test.,
checkHotFixes.String.3	The service pack level is not relevant to this test.,
checkHotFixes.String.4	The %s installed are not current. Run Windows Update to install the most recent service packs and hotfixes. The missing hotfixes are: %s. You may need to run Windows Update multiple times to install all the hotfixes. Some of the hotfixes listed may be contained in a cumulative patch.,
checkHotFixes.String.5	All required %s are installed.,
checkHotFixes.String.6	There are no %s installed. Run Windows Update to install the most recent service packs and hotfixes. You may need to run Windows Update multiple times to install all the hotfixes.,
checkIESecurityZoneSettings.String.1	There was no security zone specified.,
checkIESecurityZoneSettings.String.2	Internet Explorer %s security zone settings are acceptable.,
checkIESecurityZoneSettings.String.3	There was no security level specified.,
checkIESecurityZoneSettings.String.4	An invalid security level '%s' was specified.,
checkIESecurityZoneSettings.String.5	Could not test Internet Explorer %s security zone settings. On Windows 2000 you must be logged in as the same user that is currently being tested.,

Table 5-1.Default Test Names and Descriptions (cont.)

Test name	Description
checkIESecurityZoneSettings.String.6	The required security level for your Internet Explorer %s security zone is %s or greater. To change the setting, select Tools>>Internet Options>>Security>>%s>> select the setting and click OK. If you are using a custom setting, higher security settings are required for: %s * indicates an Internet Explorer 6 or later setting,
checkIESecurityZoneSettings.String.7	There were no Internet Explorer %s security zone settings found.,
checkIEVersion.String.1	Unable to retrieve IE version.,
checkIEVersion.String.2	Internet Explorer version %s is acceptable.,
checkIEVersion.String.3	The required Internet Explorer browser was not found or is not current. Install the latest version.,
checkMicrosoftOfficeMacroSecurityLevel.String.1	The office_program and the security_level_required parameters are required.,
checkMicrosoftOfficeMacroSecurityLevel.String.2	The specified office_program or security_level_required values are invalid.,
checkMicrosoftOfficeMacroSecurityLevel.String.3	There are no Microsoft Office products installed or the user is not logged in as the same user that is being tested.,
checkMicrosoftOfficeMacroSecurityLevel.String.4	All macro settings are acceptable.,
checkMicrosoftOfficeMacroSecurityLevel.String.5	Microsoft Office %s is not installed.,
checkMicrosoftOfficeMacroSecurityLevel.String.6	The Microsoft %s macro security level setting must be set to %s or above. To change the security level, open %s and do the following: Select \'Options...\' under the \'Tools\' menu. Choose the \'Security\' tab. Press the \'Macro Security...\' button. Select the \'Security Level\' tab. Finally, select the security level %s or higher.,
checkNetBiosInfo.String.1	An unsupported operating system was encountered.,
checkPersonalFirewalls.String.1	The required personal firewall software was not found. Install a personal firewall and keep it up-to-date. Supported firewall software: %s,
checkPersonalFirewalls.String.2	%s is installed but not running.,
checkPersonalFirewalls.String.3	%s service is installed and running.,
checkServicePacks.String.1	An unsupported operating system was encountered.,
checkServicePacks.String.2	The OS is not relevant to this test.,

Table 5-1.Default Test Names and Descriptions (cont.)

Test name	Description
checkServicePacks.String.3	There are no service packs installed. Run Windows Update to install the most recent service packs.,
checkServicePacks.String.4	There are no service packs installed. Run Windows Update to install the most recent service packs.,
checkServicePacks.String.5	All required service packs are installed,
checkServicePacks.String.6	The service packs installed are not current. Run Windows Update to install the most recent service packs. The current installed service pack is %s. You must be running service pack %s or later.,
checkServicesNotAllowed.String.1	All services found are allowed.,
checkServicesNotAllowed.String.2	The following services are not allowed: %s. Stop the service by selecting Control Panel>>Administrative Tools (located in the Performance and Maintenance category folder)>>Services application>>right-click on the service and select properties. Change the startup type to manual and click stop. Click OK to save your changes.,
checkServicesNotAllowed.String.3	%s, # placeholder for link location for each service.
checkServicesRequired.String.1	All required services were found.,
checkServicesRequired.String.2	The following required services were not found: %s. Start the service by selecting Control Panel>>Administrative Tools>>Services application>>right-click on the service and select properties. Change the startup type to automatic and click start. Click OK to save your changes. If the service does not exist contact your administrator.,
checkServicesRequired.String.3	%s, # placeholder for link location for each service.
checkSoftwareNotAllowed.String.1	Could not import the re module required by this test.,
checkSoftwareNotAllowed.String.2	All software found is allowed.,
checkSoftwareNotAllowed.String.3	Do not specify the HKEY_LOCAL_MACHINE\SOFTWARE registry key.,
checkSoftwareNotAllowed.String.4	The following software is not allowed: %s. Uninstall the software listed. Also, remove any file types listed by double-clicking My Computer>>select Tools>>Folder Options>>File Types and remove the file type mentioned.,
checkSoftwareNotAllowed.String.5	%s, # placeholder for link location for each software package.
checkSoftwareRequired.String.1	Could not import the re module required by this test.,

Table 5-1.Default Test Names and Descriptions (cont.)

Test name	Description
checkSoftwareRequired.String.2	All required software is installed.,
checkSoftwareRequired.String.3	The required software was not found: %s.,
checkSoftwareRequired.String.4	%s, # placeholder for link location for each software package.
checkUniqueId.String.1	An unsupported operating system was encountered.,
checkUniqueId.String.2	Could not determine unique ID,
checkWindowsSecurityPolicy.String.1	All Windows security policies are acceptable.,
checkWindowsSecurityPolicy.String.2	An unsupported operating system was encountered.,
checkWindowsSecurityPolicy.String.3	The OS is not relevant to this test.,
checkWindowsSecurityPolicy.String.4	The security setting required parameter '%s' is invalid,
checkWindowsSecurityPolicy.String.5	The following Windows security policies are configured incorrectly: %s. Set the Windows security policies by selecting Start>>Control Panel>>Administrative Tools>>Local Security Policy>>Local Policy>>Security Options>>double-click the policy and select enable or disable.,
checkWindowsStartupRegistryEntriesAllowed.String.1	All Windows startup registry entries are acceptable.,
checkWindowsStartupRegistryEntriesAllowed.String.2	The following Windows startup registry entries are not allowed in the HKEY_LOCAL_MACHINE>>Software>>Microsoft>>Windows Run and RunOnce registry keys: %s. Contact your network administrator for removal of these items from the registry.,
checkWormsVirusesAndTrojans.String.1	No worms, viruses or trojans were found.,
checkWormsVirusesAndTrojans.String.2	The following worms, viruses, or trojans were found: %s. Contact your network administrator for assistance on removing them.,
checkAntiSpyware.String.1	The %s software is installed and a scan was run recently on %s.,
checkAntiSpyware.String.2	The %s software was found but a scan has not performed within the last %s days.,
checkAntiSpyware.String.3	The required anti-spyware software was not found. Supported anti-spyware software: %s,
checkAntiSpyware.String.4	The %s software was found but a signature update has not been performed within the last %s days.,

Table 5-1.Default Test Names and Descriptions (cont.)

Test name	Description
checkAntiSpyware.String.5	The %s software was found but a scan has never been performed.,
checkBadIP.String.1	There were no unauthorized network connections found.,
checkBadIP.String.2	An unsupported operating system was encountered.,
checkBadIP.String.3	The IP addresses %s are on unauthorized networks.,
checkBadIP.String.4	The IP address %s is on an unauthorized network.,

Table 5-1.Default Test Names and Descriptions (cont.)

6

NAC Policies

Chapter Contents

Overview 6-2
Standard NAC Policies 6-4
NAC Policy Group Tasks 6-5
- Add a NAC Policy Group 6-5
- Editing a NAC Policy Group 6-5
- Deleting a NAC Policy Group 6-6

NAC Policy Tasks 6-7
- Enabling or Disabling an NAC Policy 6-7
- Selecting the Default NAC Policy 6-7
- Creating a New NAC Policy 6-7
- Editing a NAC Policy 6-12
- Copying a NAC Policy 6-12
- Deleting a NAC Policy 6-13
- Moving a NAC Policy Between NAC Policy Groups 6-13
- Assigning Endpoints and Domains to a Policy 6-13
- NAC Policy Hierarchy 6-14
- Setting Retest Time 6-14
- Setting Connection Time 6-14
- Defining Non-supported OS Access Settings 6-15
- Setting Test Properties 6-15
- Selecting Action Taken 6-15

About NAC 800 Tests 6-17
- Viewing Information About Tests 6-17
- Selecting Test Properties 6-17
- Test Icons 6-19

Overview

"NAC policies" are collections of tests that evaluate remote endpoints attempting to connect to your network. You can use the standard tests installed with NAC 800, or you can create your own custom tests.

NOTE:

The default NAC policy is indicated by the check mark on the icon to the left of the NAC policy name. See “Selecting the Default NAC Policy” on page 6-7 for instructions on selecting and charging the default NAC policy.

The **NAC policies** window (shown in figure 6-1) is where you create NAC policies and groups, disable NAC policies, delete NAC policies, access specific NAC policies. Once you access a specific policy, you can perform the following tasks:

- **Basic settings** – Edit NAC policies, assign NAC policies to a group, enable or disable the NAC policy, select which OSs are not tested, but allowed access, set retest frequency, and set quarantine times.
- **Domains and endpoints** – Assign endpoints and domains to a policy.
- **Tests** – Select tests, select test properties, select test failure actions.

To view the NAC policies window:

NAC 800 Home window>>NAC policies

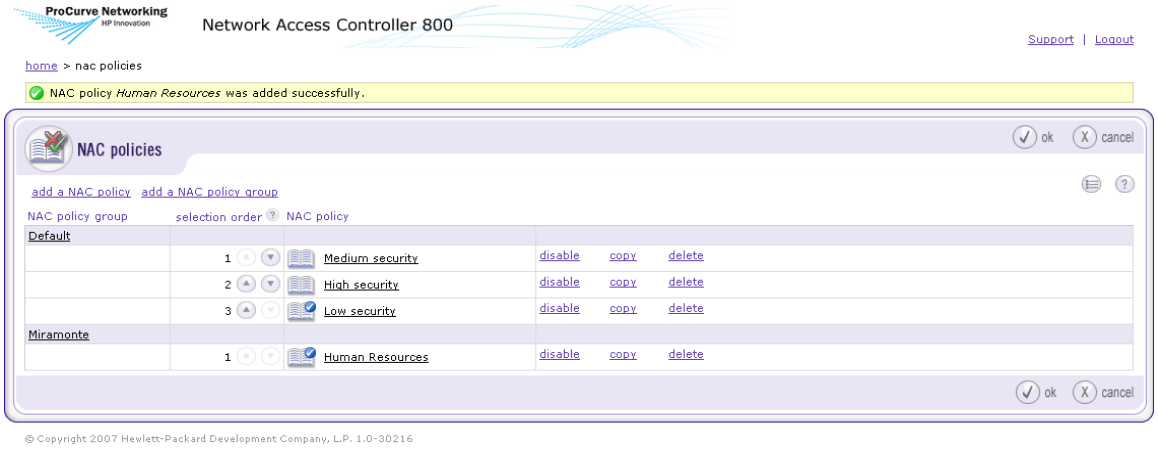


Figure 6-1. NAC Policies Window

The following figure shows the legend explaining the NAC policies icons:

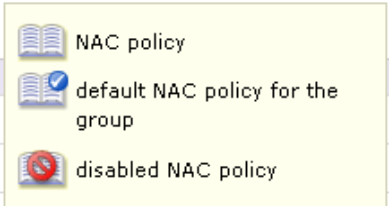


Figure 6-2. NAC Policies Window Legend

Standard NAC Policies

NAC 800 ships with three standard NAC policies:

- High security
- Low security
- Medium security

NAC policies are organized in groups, which include the clusters defined for your system, a **Default** group, and any other groups you create. Each standard policy has tests pre-selected. You can modify these policies, or create custom policies.

NAC Policy Group Tasks

Add a NAC Policy Group

To add an NAC policy group:

NAC 800 Home window>>NAC policies

1. Click **Add an NAC policy group**. The **Add NAC policy group** window opens:

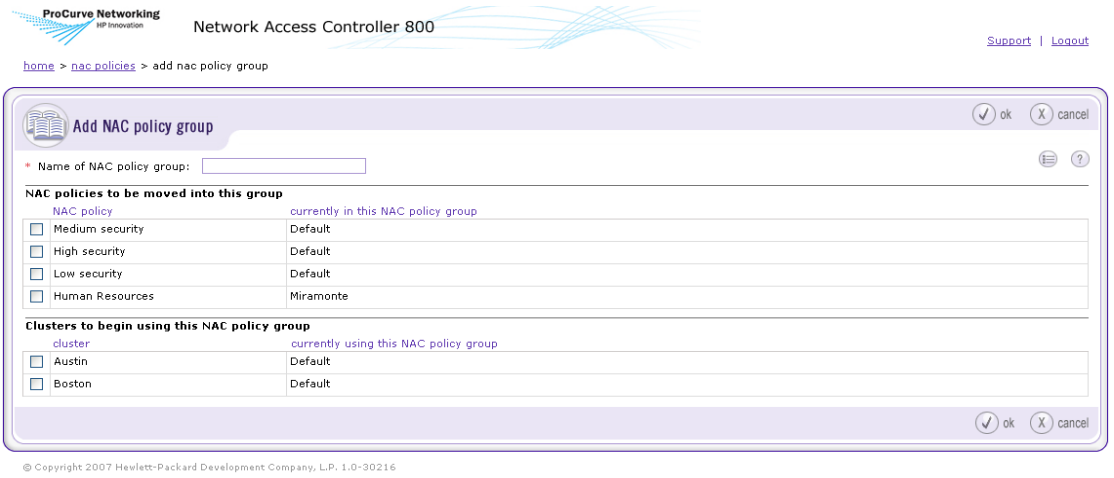


Figure 6-3. Add NAC Policy Group Window

2. Type a name for the group in the **Name of NAC policy group** text box.
3. Optional: Select the check box next to any NAC policy to move to this group.
4. Optional: Select the check box next to any cluster to move to this group.
5. Click **ok**.

Editing a NAC Policy Group

To edit an existing NAC policy group:

NAC 800 Home window>>NAC policies

1. Click on an existing NAC policy group name (for example, **Default**). The **NAC policy group** window opens.

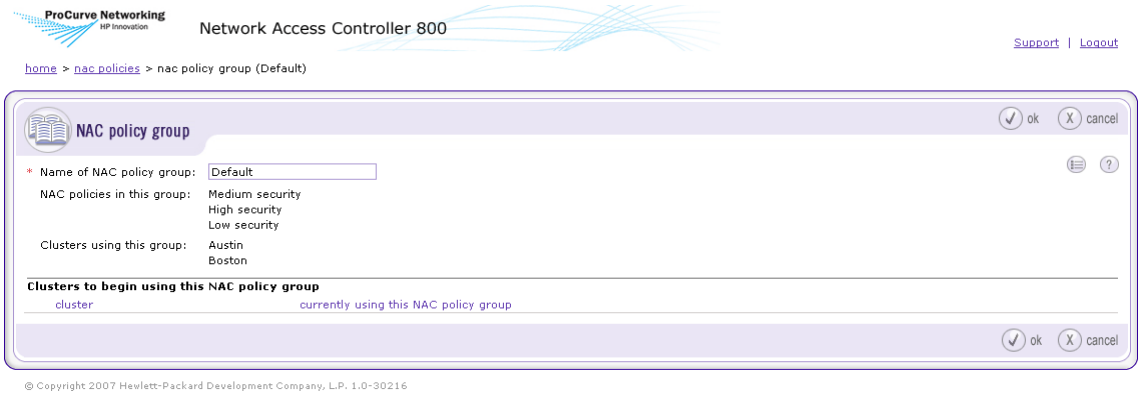


Figure 6-4. Edit NAC Policy Group Window

2. Make any changes required. See "Add a NAC Policy Group" on page 6-5 for details on NAC policy group options.
3. Click **OK** to save or **Cancel** to return without saving.

Deleting a NAC Policy Group

To delete a NAC policy group:

NAC 800 home window>>NAC policies

NOTE: You cannot delete a NAC policy group if any clusters are using it; first, you need to assign a different NAC policy group to all of the clusters from the **System configuration>>Enforcement clusters & servers** window.

1. Select **delete** next to the NAC policy group you want to delete. A confirmation window appears.
2. Click **yes** on the **Delete NAC policy group** confirmation window.

NAC Policy Tasks

Enabling or Disabling an NAC Policy

Select which NAC polices are enabled or disabled.

To enable/disable a NAC policy:

NAC 800 Home window>>NAC policies

Click on the **enable** or **disable** link. An X indicates disabled.

Selecting the Default NAC Policy

To select the default NAC policy:

NAC 800 Home window>>NAC policies

Click on the up or down arrow to move the NAC policy. The default NAC policy is the one toward the bottom of the list with the highest selection number as shown in the following figure:

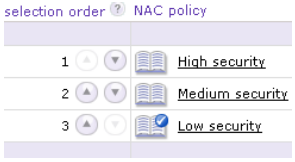


Figure 6-5. Default NAC Policy

Creating a New NAC Policy

Create custom policies that are based on existing policies, or create new policies from scratch.

To create a new NAC policy:

NAC 800 Home window>>NAC policies

1. Click **Add a NAC policy**. The **Add a NAC policy** window opens as shown in the following figure:

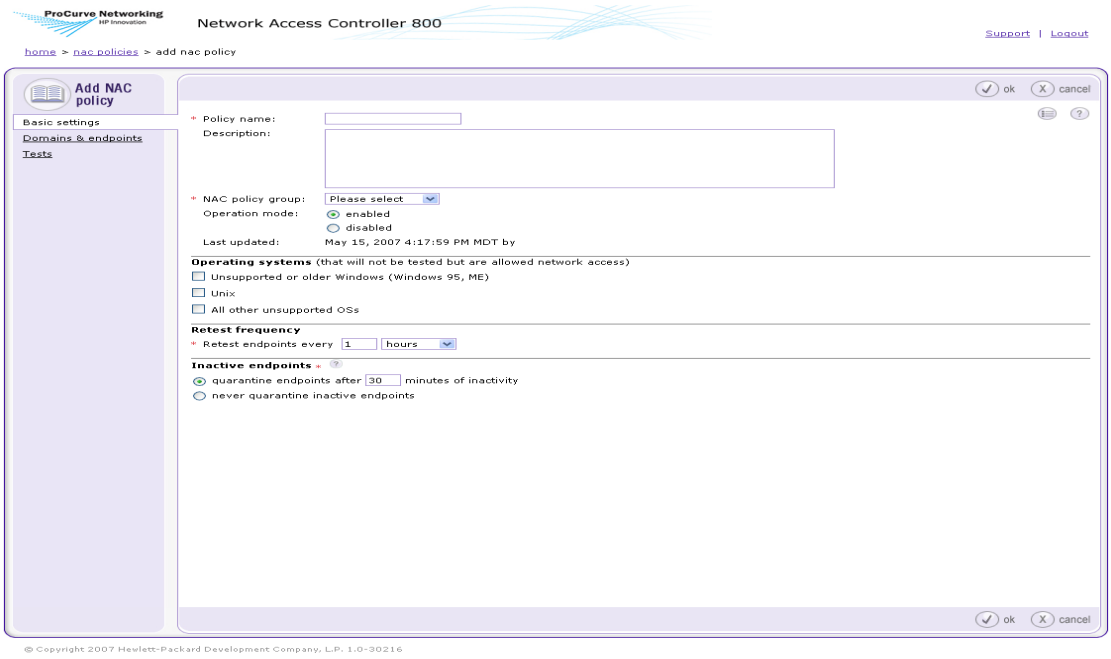


Figure 6-6. Add an NAC Policy, Basic Settings Area

2. Enter a policy name.
3. Enter a description in the **Description** text box.
4. Select a **NAC policy group**.
5. Select either the **enabled** radio button or the **disabled** radio button.
6. Select the **Operating systems** that will not be tested but are allowed network access.
   - **Unsupported or older Windows (Windows 95 or ME)**
   - **UNIX**
   - **All other unsupported OSs**

NOTE: In DHCP mode, if an endpoint with an unsupported OS already has a DHCP-assigned IP address, NAC 800 cannot affect this endpoint in any way until the lease on the existing IP address for that endpoint expires. If an endpoint with an unsupported OS has a static IP address, NAC 800 cannot affect this

endpoint in any way. In both of these cases, the System Monitor window may show the quarantined icon next to these endpoints; however, if you hover your mouse over the red circle, the actual status shows that the endpoint should be quarantined, but the quarantine action was unsuccessful.

CAUTION: Allowing untested endpoints on your network contains risks. See "Untestable Endpoints and DHCP Mode" on page 7-18 for more information.

7. In the **Retest frequency area**, enter how frequently NAC 800 should retest a connected machine.

TIP: A lower number ensures higher security, but puts more load on the NAC 800 server.

8. In the **Inactive endpoints area**, enter how long an end-user can be inactive before they have to log in again. To allow end-users to remain connected indefinitely select **never quarantine inactive endpoints**.
9. Click the **Domains and endpoints** menu option to open the **Domains and endpoints** window, shown in the following figure:

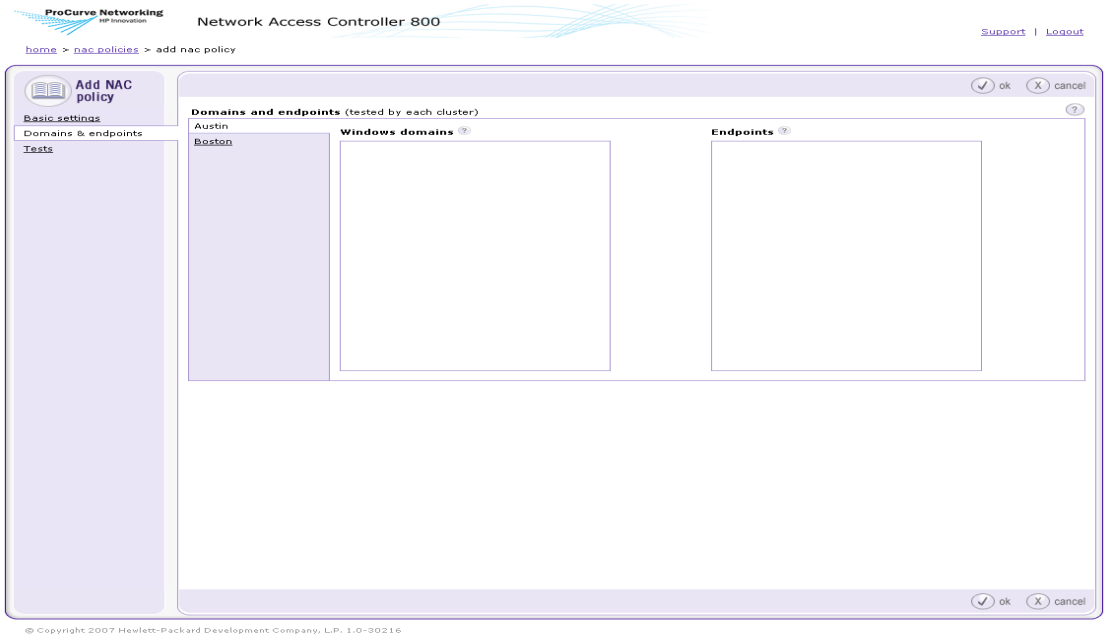


Figure 6-7. Add an NAC Policy, Domains and Endpoints Window

10. Click on a cluster name.
11. Enter the names of Windows domains to be tested by this cluster for this NAC policy, separated by a carriage return.
12. Enter a single endpoint or list of endpoints separated by a carriage return using the endpoint IP address, MAC address, NetBIOS name, or host name. Enter a range of IPs using a dash (-) between or by using CIDR notation (see table 13-1, “CIDR Naming Conventions,” on page 13-9).

NOTE: You can leave the Domains and Endpoints areas blank if you do not want to assign domains and endpoints to this policy.

TIP: Move the mouse cursor over the question mark (?) by the word Endpoints, then click on the CIDR notation link to see the CIDR conversion table pop-up window.

13. Click the **Tests** menu option to open the **Tests** window:

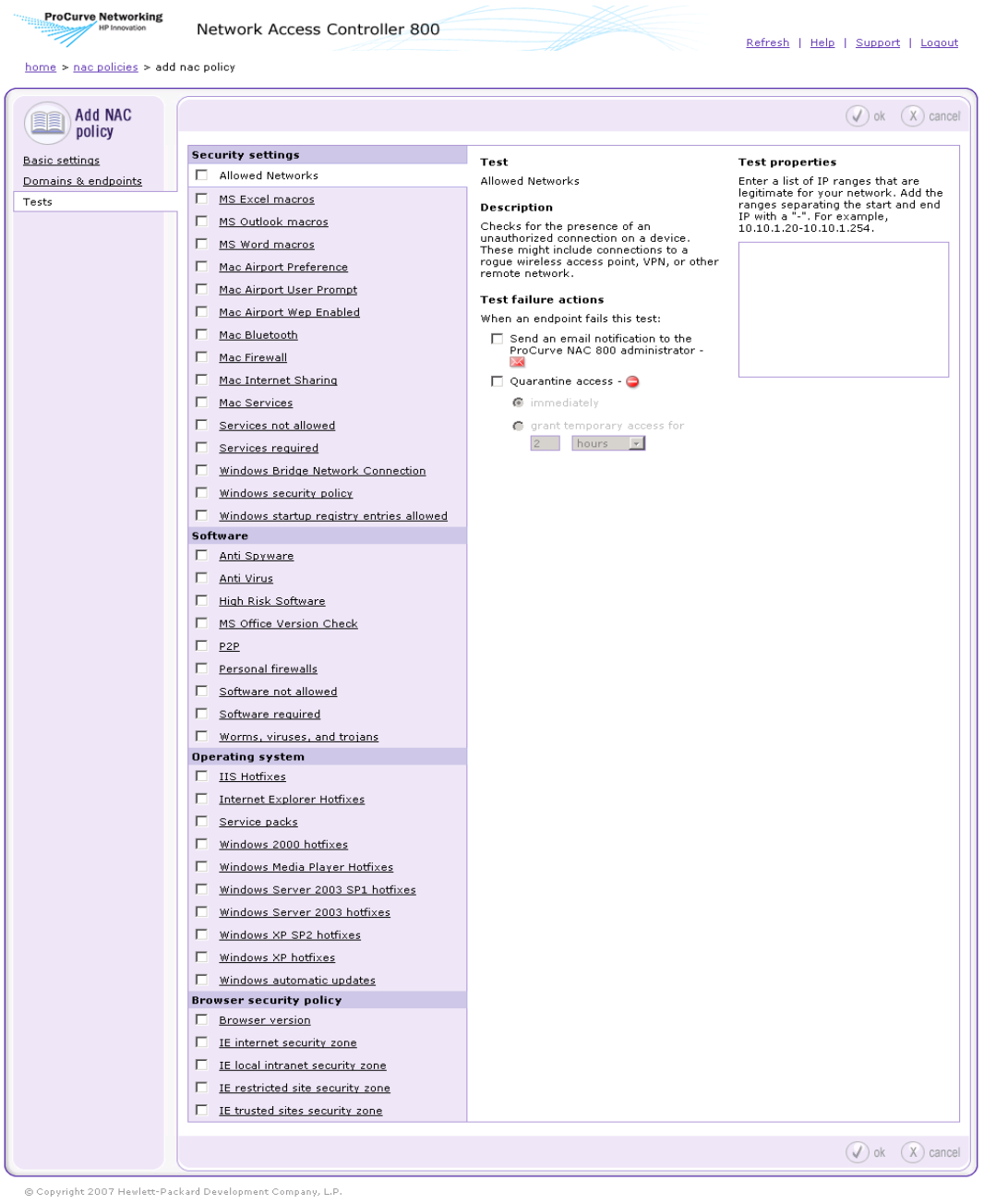


Figure 6-8. Add NAC Policy, Tests Area

14. Select a test to include in the NAC policy by clicking on the check box next to the test name.
15. Select a test by clicking on the test name to view the properties. For more information about test properties, see “Selecting Test Properties” on page 6-17.
16. Select the test properties for this test. For more information about the specific tests, see “Tests Help” on page A-1.
17. Select an action to take when an endpoint fails this test (see “Selecting Action Taken” on page 6-15).
18. Click **ok**.

TIP: Selecting the **Send an email notification** option sends an email to the address you identified in **NAC 800 Home window>>System Configuration>>Notifications** area. This option is defined per cluster.

Editing a NAC Policy

To edit an existing NAC policy:

NAC 800 home window>>NAC policies

1. Click on a **NAC policy** name.
2. Change any of the options desired. See “Creating a New NAC Policy” on page 6-7 for details on the options available.
3. Click **ok**.

Copying a NAC Policy

To copy an existing NAC policy:

NAC 800 Home window>>NAC policies

1. Click the **copy** link to the right of the NAC policy you want to copy.
2. Enter a new NAC policy name.
3. Change any of the options desired. See “Creating a New NAC Policy” on page 6-7 for details on the options available.
4. Click **ok**.

Deleting a NAC Policy

To delete an existing NAC policy:

NAC 800 Home window>>NAC policies

1. Click the **delete** link to the right of the NAC policy you want to delete. A confirmation window appears.
2. Click **yes**.

Moving a NAC Policy Between NAC Policy Groups

To move a NAC policy between NAC policy groups:

NAC 800 Home window>>NAC policies

1. To open the **NAC policies** window, click a **NAC policy** name.
2. Select a new NAC policy group from the **NAC policy group** drop-down list.
3. Click **ok**.

Assigning Endpoints and Domains to a Policy

Select which endpoints are associated with each policy.

To assign endpoints and domains to a policy:

NAC 800 Home window>>NAC policies>>Select a NAC Policy>>Domains and endpoints menu option

1. Enter a single endpoint or list of endpoints separated by a carriage return using the endpoint IP address, MAC address, or NetBIOS name. Enter a range of IPs using a dash (-) between them, or by using CIDR notation (see “Entering Networks Using CIDR Format” on page 13-9).
2. In the **Windows domains** area, enter a domain name or list of domain names separated by a carriage return.
3. Click **ok**.

NOTE: Adding an endpoint or domain to multiple policies results in the endpoint being assigned to the first enabled NAC policy in the list.

NAC Policy Hierarchy

If an endpoint is listed in more than one NAC policy, the order of use is as alphabetical by name of NAC policy (not including the default NAC policy).

Setting Retest Time

Retest endpoints connected to your network frequently to guard against potential changes in the remote endpoint configurations.

To set the time to wait before retesting a connected endpoint:

NAC 800 Home window>>NAC policies>>Select a NAC Policy>>Basic settings menu option

1. In the **Retest frequency area**, enter how frequently in minutes, hours, or days NAC 800 should retest a connected endpoint.

TIP: A lower number ensures higher security, but puts more load on the NAC 800 server.

2. Click **ok**.

Setting Connection Time

Disconnect end-users after a specific amount of time to guard against other parties accessing the connection while the authenticated end-user has stepped away from their desk.

To set the time an end-user can be inactive before requiring the end-user to log in again:

NAC 800 Home window>>NAC policies>>Select a NAC Policy>>Basic settings menu option

1. In the **Inactive endpoints area**, enter how long an end-user can be inactive before they have to log in again.

TIP: A lower number ensures higher security.

2. Click **ok**.

Defining Non-supported OS Access Settings

To define what actions to take for endpoints with non-supported operating systems:

Main NAC 800 window>>NAC policies>>Select a NAC Policy>>Basic settings area

1. In the **Operating systems** area, select the check box beside any operating system that you will allow access without being tested.
2. Click **ok**.

Setting Test Properties

Test properties are specific to the particular test. Select the properties you want applied. Tests are explained in detail in "Tests Help" on page A-1.

To set the test properties for a specific test:

NAC 800 Home window>>NAC policies>>Select a NAC Policy>>Tests menu option

1. Click on the name of test to display the test's options.

NOTE: Click a test name to display the options; select the test check box to enable the test for the policy you are modifying.

2. Select the test failure actions to apply for this test:
   - **Send email notification**
   - **Quarantine access**
3. Select any test properties if applicable.
4. Click **ok**.

Selecting Action Taken

Actions can be passive (send an email), active (quarantine) or a combination of both.

To select the action to take:

NAC 800 Home window>>NAC policies>>Select a NAC Policy>>Tests menu option

1. Click on the name of test to display the test's options.

NOTE: Click a test name to display the options; select the test check box to enable the test for the policy you are modifying.

2. Select an action to take when an endpoint fails this test.
   a. **Send an email notification...** – sends an email to the email address specified (see "Notifications" on page 3-102).

NOTE: An email is sent for each retest.

   b. **Quarantine access** – specify when the endpoint should be denied access.
      i. **immediately**
      ii. **grant temporary access...**

      If you select a temporary access period here, the end-users are allowed temporary access for the specified time, after which they are denied access until they pass the test. The temporary access period allowed is shown on the end-user results window (see "End-user Access" on page 5-1).

TIP: The minimum amount of time you can grant temporary access is 10 minutes.

3. Click **ok**.

About NAC 800 Tests

NAC 800 tests are assigned to NAC policies. NAC policies are used to test endpoints attempting to connect to your network. NAC 800 tests might be updated as often as hourly; however, at the time of this release, the tests shown in "Tests Help" on page A-1 were included (see "Viewing Information About Tests" on page 6-17 for instructions on viewing the latest list of tests).

Viewing Information About Tests

To view the most current list of tests and descriptions:

NAC 800 Home window>>NAC policies>>Select a NAC Policy>>Tests menu option

Click on a test name. The test description and selectable properties are shown for the selected test.

If the icons (Figure 6-9 on page 6-19) are red, the test is enabled and the actions selected will take effect immediately. If the icons are gray, the test is not enabled, and the actions will not take effect. To enable the test, select the check box next to the test name.

Selecting Test Properties

Tests either have standard properties (non-selectable), selectable properties, or text entry fields.

Select the check box or radio button that applies for each test. A check box indicates that you can make multiple selections. A radio button indicates that you can make one choice from the list.

Entering Software Required/Not Allowed

NAC 800 checks the Windows registry on the endpoint for the existence of software. Most software vendors record their product information in the `HKEY_LOCAL_MACHINE\Software` registry key using the following format:

```
<vendor>\<software package>\<version>
```

For example, `Mozilla\Mozilla Firefox 1.5.0.6`

You can enter any combination of these keys in the NAC 800 text entry fields to detect a vendor, software package and version on an endpoint (for example, you can also enter `Mozilla\Firefox` or simply `Mozilla`) and NAC 800 searches for them in the `HKEY_LOCAL_MACHINE\Software` registry key sub-tree.

TIP: The entries are not case sensitive. This test simply checks to see if the registry key exists in HKEY_LOCAL_MACHINE\Software or HKEY_CURRENT_USER\Software. So, these values must match the registry keys as displayed in the registry editor. If you just specify Mozilla and HKEY_LOCAL_MACHINE\Software\Mozilla exists in the registry, the test would match.

To find the software registry keys on the endpoint:

1. Select **Start>>Run**
2. Type:
   `regedit`
3. Click **OK**.
4. Expand the `HKEY_LOCAL_MACHINE` key.
5. Expand the Software key.
6. View the sub-trees for various vendors software and versions.

TIP: If you're looking for a registry key, you enter a trailing slash. If you're looking for a registry value, you do not enter a trailing slash.

Entering Service Names Required/Not Allowed

Services are Windows operating system applications that run automatically, without manual intervention.

To find the services names on the endpoint:

Service names must be entered exactly as they appear in **Control panel>>Administrative tools>>Services application**.

TIP: Enter the names of software and services in the NAC 800 text entry field separated by a carriage return.

For example, the following are examples of services:

- Telnet

- Utility Manager
- Windows Installer

Entering the Browser Version Number

To specify the minimum browser version the end-user needs:

1. For Mozilla Firefox:
   a. Clear the **Check For Mozilla Firefox [1.5]** check box.
   b. Type a version number in the text entry field.
2. For Internet Explorer on Windows XP and Windows 2003:
   a. Clear the **Check For Internet Explorer for Windows XP and Windows 2003 [6.0.2900.2180]** check box.
   b. Type a version number in the text entry field.
3. For Internet Explorer on Windows 2000:
   a. Clear the **Check For Internet Explorer for Windows 2000 [6.0.2800.1106]** check box.
   b. Type a version number in the text entry field.

Test Icons

The NAC policy tests show icons that represent the test failure action selected as shown in the following figure:

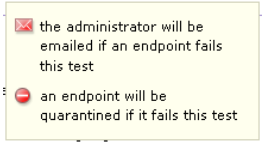


Figure 6-9. NAC Policy Test Icons

(This page intentionally left blank.)

Quarantined Networks

Chapter Contents

Endpoint Quarantine Precedence 7-2
Using Ports in Accessible Services and Endpoints 7-4
Determining Accessible Services Example 7-6
Always Granting Access to an Endpoint 7-13
Always Quarantining an Endpoint 7-15
New Users 7-16
Shared Resources 7-17
Untestable Endpoints and DHCP Mode 7-18

Endpoint Quarantine Precedence

Endpoints are quarantined in the following hierarchical order:

1. **Access mode** (normal operation, quarantine all, or allow all)
2. **Temporarily quarantine for/Temporarily grant access for** radio buttons
3. **Endpoint testing exceptions** (always grant access, always quarantine)
4. **NAC policies**

NOTE: In DHCP mode, if an endpoint with an unsupported OS already has a DHCP-assigned IP address, NAC 800 cannot affect this endpoint in any way until the lease on the existing IP address for that endpoint expires. If an endpoint with an unsupported OS has a static IP address, NAC 800 cannot affect this endpoint in any way. In both of these cases, the System Monitor window may show the quarantined icon next to these endpoints; however, if you hover your mouse over the red circle, the actual status shows that the endpoint should be quarantined, but the quarantine action was unsuccessful.

The following describes the process in more detail:

- **Access mode** (1) overrides the items below it in the previous list (2, 3, and 4). Use the **Access mode** radio buttons (**System monitor>>select a cluster**) to act globally on all endpoints in an Enforcement cluster.
- The **Temporarily quarantine for/Temporarily grant access for** radio buttons (**Endpoint activity>>select an endpoint check box>>Change access**) override the items below them in the list (3 and 4).

  Use **Temporarily quarantine for** to temporarily quarantine endpoints that:
  - Have been designated **Always grant access and never test** (**System configuration>>Exceptions**)
  - Are defined in NAC policies and have passed tests

  Use **Temporarily grant access for** to allow temporary access to endpoints that:
  - Have been designated **Always quarantine and never test** (**System configuration>>Exceptions**).
  - Are defined in NAC policies and have failed tests

TIP: Use the **Clear temporary access control status** radio button to remove the temporary access or temporary quarantine state enabled by the **Temporarily quarantine for/Temporarily grant access for** radio buttons.

- **Endpoint testing exceptions** overrides items following it in the list (4). Use **Endpoint testing exceptions** (**System configuration>>Exceptions**) to always allow or always quarantine endpoints that are defined in NAC policies. For example, an NAC policy might have a range of IP addresses defined for testing, but you want to exclude specific IP addresses within that range from the tests, so you could specify them here as **Always grant access and never test** or **Always quarantine and never test**.

TIP: The change access button on the System Configuration>>Endpoint activity window is enabled only when the action is possible; for example, when an endpoint or endpoints are selected.

Using Ports in Accessible Services and Endpoints

To use a port number when specifying accessible services and endpoints (cluster default):

NAC 800 Home window>>System configuration>>Accessible services

The following figure shows the **Accessible services** window:

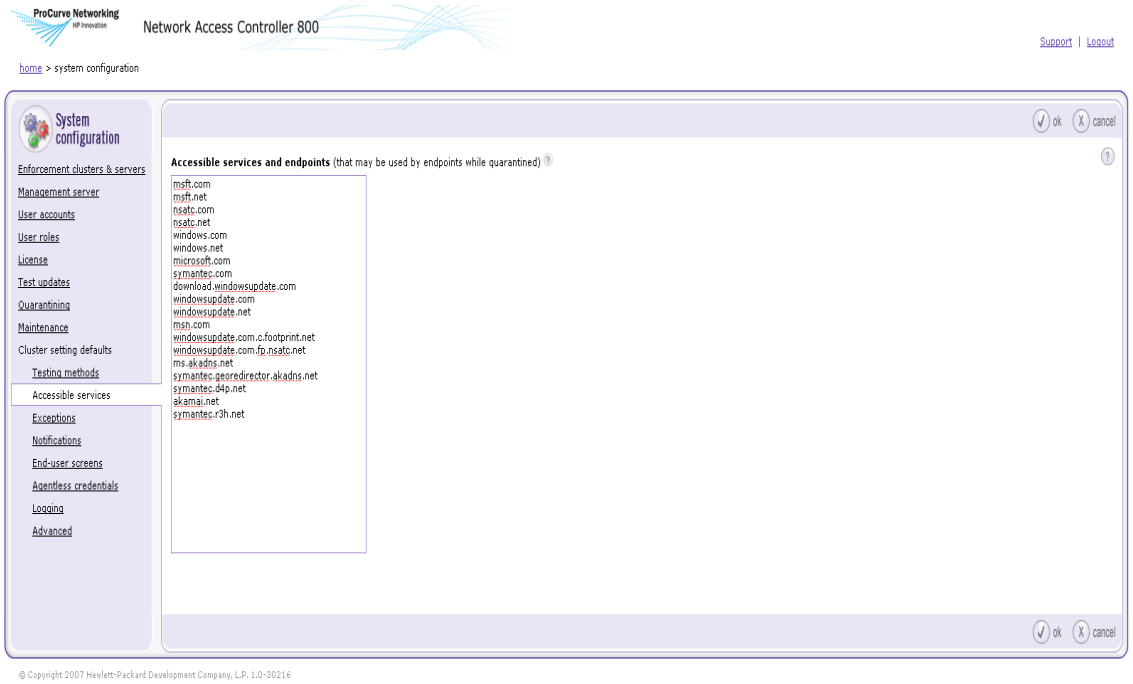


Figure 7-1. Accessible Services Window

In order to grant access for quarantined endpoints to needed services, add entries to the **Accessible services** list. For inline enforcement mode, enter the IP addresses of the servers that provide the services. A port or ports can be added to limit the access to the servers from quarantined endpoints.

For all other deployment modes, the Fully Qualified Domain Name (FQDN) of the target servers should be added to the list (for example mycompany.com). If the specified servers are not behind an ES, a network firewall must be used to control access to only the desired ports.

1. For inline enforcement mode, in the **Accessible services and endpoints** area, enter an endpoint followed by a colon (:), followed by a port number as shown as follows:
   ```
   10.0.16.100:53
   ```

   Separate multiple endpoint entries with a carriage return (new line):

   ```
   10.0.16.100:53
   10.0.16.100:80
   10.0.16.100:81
   10.0.16.100:82
   ```
2. Click **ok**.

NOTE: Enter a range of ports as follows:
10.0.16.100:53:65

Determining Accessible Services Example

Determining which services to add in the **Accessible services** area can be tricky. This section details the steps used to determine all of the accessible services required to allow a quarantined endpoint to access the Windows Update service and retrieve the required service packs and/or hotfixes.

The following setup is used for this example:

- An endpoint that is currently quarantined, or uses the NAC 800 ES as its DNS server
- SSH access to the NAC 800 ES
- Access to the NAC 800 MS console (user interface)
- Access to the endpoint trying to access the Windows Update service

To determine the required accessible services:

1. Log into as `root` to the ES using an SSH client such as PuTTY (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html).
2. Enter the following command:

   ```
   tcpdump -i eth0 -s0 port 53 and host 172.21.20.20
   ```

   Where:
   `host` is the endpoint

   You can also use the `-w` flag to output this to a file and view with WireShark (http://www.wireshark.org/).
3. Log into the endpoint, open a browser window, and attempt to go to the Windows Update page (http://update.microsoft.com). Data is produced in the SSH window to the ES.
4. In the SSH window to the ES, the `tcpdump` for this example was as follows:

   ```
   16:20:22.551309 IP 172.21.20.20.2586 > SA00.domain:
   49734+ A? windowsupdate.microsoft.com. (45)

   16:20:22.552492 IP SA00.domain > 172.21.20.20.2586:
   49734 NXDomain* 0/1/0 (96)
   ```

```
16:20:50.529861 IP 172.21.20.20.2586 > SA00.domain:
40773+ A? windowsupdate.microsoft.com. (45)

16:20:50.531469 IP SA00.domain > 172.21.20.20.2586:
40773 NXDomain* 0/1/0 (96)
```

5. Log into the NAC 800 MS console using an administrator account.
6. Navigate to the **Accessible services** window (**System configuration>>Accessible services**).
7. Add **microsoft.com** to the accessible services and endpoints list.
8. Click **OK**.
9. On the endpoint, clear the temporary files. For Internet Explorer, select **Tools>>Internet Options>>Delete Files** as shown in the following figure.

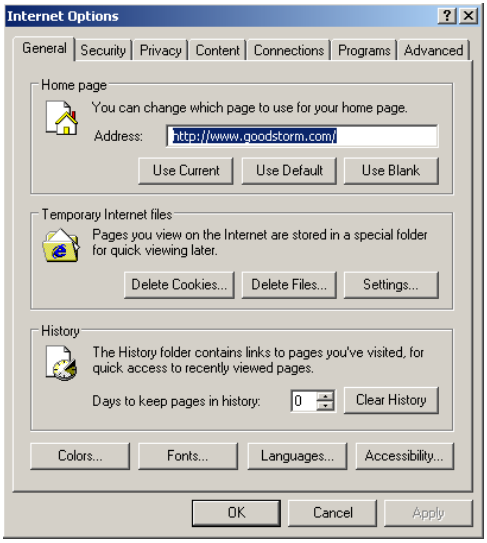


Figure 7-2. Clear Temporary Tiles Window

10. Repeat step 3 through step 9 until the endpoint can successfully download service packs and hotfixes from the Windows Update service.

The final list of accessible services for this example is shown in the following figure.

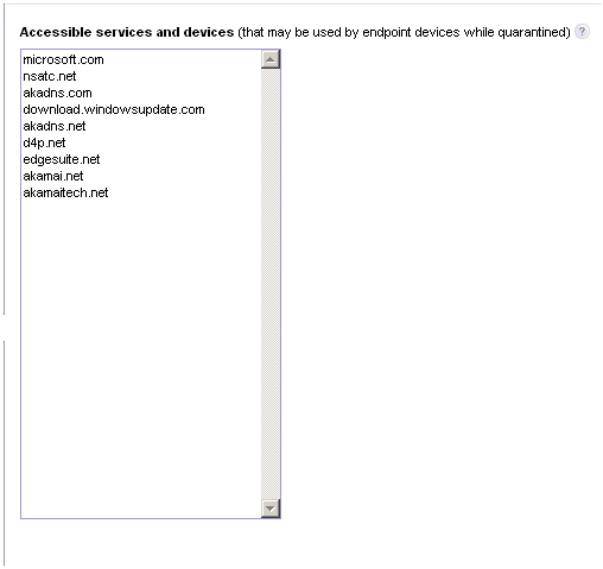


Figure 7-3. Final List of Accessible Services Example

The complete `tcpdump` results for this example are shown below:

```
tcpdump -i eth0 -s0 -w /tmp/dns.pcap  port 53 and host 172.21.20.20


waldo:~ # tcpdump -i eth0 -s0 port 53 and host 172.21.20.20
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes



16:20:22.551309 IP 172.21.20.20.2586 > SA00.domain:  49734+ A?
      windowsupdate.microsoft.com. (45)
16:20:22.552492 IP SA00.domain > 172.21.20.20.2586:  49734 NXDomain* 0/1/0 (96)
16:20:50.529861 IP 172.21.20.20.2586 > SA00.domain:  40773+ A?
      windowsupdate.microsoft.com. (45)
16:20:50.531469 IP SA00.domain > 172.21.20.20.2586:  40773 NXDomain* 0/1/0 (96)



16:22:07.387959 IP 172.21.20.20.2586 > SA00.domain:  12107+ A?
      windowsupdate.microsoft.com. (45)
16:22:07.491558 IP SA00.domain > 172.21.20.20.2586:  12107 2/1/1 CNAME
      windowsupdate.microsoft.nsatc.net., A SA00 (148)
```

```
16:23:56.240873 IP 172.21.20.20.2586 > SA00.domain:  55115+ A?
      windowsupdate.microsoft.com. (45)
16:23:56.245644 IP SA00.domain > 172.21.20.20.2586:  55115 2/7/7 CNAME
      windowsupdate.microsoft.nsatc.net., A 207.46.225.221 (353)
16:23:56.981306 IP 172.21.20.20.2586 > SA00.domain:  34378+ A?
      update.microsoft.com. (38)
16:23:56.981667 IP SA00.domain > 172.21.20.20.2586:  34378 NXDomain* 0/1/0 (89)



16:25:03.645582 IP 172.21.20.20.2586 > SA00.domain:  12872+ A?
      windowsupdate.microsoft.com. (45)
16:25:03.646869 IP SA00.domain > 172.21.20.20.2586:  12872 2/7/7 CNAME
      windowsupdate.microsoft.nsatc.net., A 207.46.225.221 (353)
16:25:04.416125 IP 172.21.20.20.2586 > SA00.domain:  11599+ A?
      update.microsoft.com. (38)
16:25:04.479209 IP SA00.domain > 172.21.20.20.2586:  11599 4/7/7 CNAME
      update.microsoft.com.nsatc.net., A 65.55.192.93, A 207.46.199.93, A
      207.46.211.126 (375)
16:25:11.580509 IP 172.21.20.20.2586 > SA00.domain:  64591+ A?
      download.windowsupdate.com. (44)
16:25:11.581118 IP SA00.domain > 172.21.20.20.2586:  64591* 1/1/1 A SA00 (100)
16:25:11.617861 IP 172.21.20.20.2586 > SA00.domain:  27470+ A?
      download.microsoft.com. (40)
16:25:12.612147 IP 172.21.20.20.2586 > SA00.domain:  27470+ A?
      download.microsoft.com. (40)
16:25:13.615052 IP 172.21.20.20.2586 > SA00.domain:  27470+ A?
      download.microsoft.com. (40)
16:25:15.619874 IP 172.21.20.20.2586 > SA00.domain:  27470+ A?
      download.microsoft.com. (40)
16:25:15.813945 IP SA00.domain > 172.21.20.20.2586:  27470 2/1/1 CNAME
      main.dl.ms.akadns.net., A SA00 (131)
16:25:15.814052 IP SA00.domain > 172.21.20.20.2586:  27470 2/1/1 CNAME
      main.dl.ms.akadns.net., A SA00 (131)
16:25:15.814152 IP SA00.domain > 172.21.20.20.2586:  27470 2/1/1 CNAME
      main.dl.ms.akadns.net., A SA00 (131)
16:25:15.814242 IP SA00.domain > 172.21.20.20.2586:  27470 2/1/1 CNAME
      main.dl.ms.akadns.net., A SA00 (131)
16:25:16.105827 IP 172.21.20.20.2586 > SA00.domain:  45902+ A? c.microsoft.com.
      (33)
16:25:16.431081 IP SA00.domain > 172.21.20.20.2586:  45902 2/1/1 CNAME
      c.microsoft.akadns.net., A SA00 (125)16:25:17.222672 IP 172.21.20.20.2586
      > SA00.domain:  4940+ A? stats.update.microsoft.com. (44)
16:25:17.338967 IP SA00.domain > 172.21.20.20.2586:  4940 2/7/7 CNAME
      statsupdate.microsoft.com.nsatc.net., A 207.46.253.219 (354)



16:27:02.834141 IP 172.21.20.20.2586 > SA00.domain:  19283+ A?
      windowsupdate.microsoft.com. (45)
16:27:02.835986 IP SA00.domain > 172.21.20.20.2586:  19283 2/7/7 CNAME
      windowsupdate.microsoft.nsatc.net., A 207.46.225.221 (353)
16:27:03.589567 IP 172.21.20.20.2586 > SA00.domain:  64338+ A?
      update.microsoft.com. (38)
16:27:03.590169 IP SA00.domain > 172.21.20.20.2586:  64338 4/7/7 CNAME
      update.microsoft.com.nsatc.net., A 207.46.211.126, A 65.55.192.93, A
      207.46.199.93 (375)
```

```
16:27:09.136659 IP 172.21.20.20.2586 > SA00.domain:  5201+ A?
      download.windowsupdate.com. (44)
16:27:09.137238 IP SA00.domain > 172.21.20.20.2586:  5201* 1/1/1 A SA00 (100)
16:27:09.172260 IP 172.21.20.20.2586 > SA00.domain:  27984+ A?
      download.microsoft.com. (40)
16:27:09.172793 IP SA00.domain > 172.21.20.20.2586:  27984 2/1/1 CNAME
      main.dl.ms.akadns.net., A SA00 (131)
16:27:09.991527 IP 172.21.20.20.2586 > SA00.domain:  5968+ A? c.microsoft.com.
      (33)
16:27:09.992035 IP SA00.domain > 172.21.20.20.2586:  5968 2/1/1 CNAME
      c.microsoft.akadns.net., A SA00 (125)
16:27:10.543332 IP 172.21.20.20.2586 > SA00.domain:  33872+ A?
      stats.update.microsoft.com. (44)
16:27:10.543984 IP SA00.domain > 172.21.20.20.2586:  33872 2/7/7 CNAME
      statsupdate.microsoft.com.nsatc.net., A 207.46.253.219 (354)



16:28:26.185059 IP 172.21.20.20.2586 > SA00.domain:  8790+ A?
      windowsupdate.microsoft.com. (45)
16:28:26.186882 IP SA00.domain > 172.21.20.20.2586:  8790 2/7/7 CNAME
      windowsupdate.microsoft.nsatc.net., A 207.46.225.221 (353)
16:28:27.725022 IP 172.21.20.20.2586 > SA00.domain:  8278+ A?
      update.microsoft.com. (38)
16:28:27.725726 IP SA00.domain > 172.21.20.20.2586:  8278 4/7/7 CNAME
      update.microsoft.com.nsatc.net., A 207.46.199.93, A 207.46.211.126, A
      65.55.192.93 (375)
16:28:39.789258 IP 172.21.20.20.2586 > SA00.domain:  18260+ A?
      download.windowsupdate.com. (44)
16:28:40.508328 IP SA00.domain > 172.21.20.20.2586:  18260 2/1/1 CNAME
      main.dl.wu.akadns.net., A SA00 (135)
16:28:40.545931 IP 172.21.20.20.2586 > SA00.domain:  36180+ A?
      download.microsoft.com. (40)
16:28:40.546463 IP SA00.domain > 172.21.20.20.2586:  36180 2/1/1 CNAME
      main.dl.ms.akadns.net., A SA00 (131)
16:28:40.906093 IP 172.21.20.20.2586 > SA00.domain:  16987+ A? c.microsoft.com.
      (33)
16:28:40.906638 IP SA00.domain > 172.21.20.20.2586:  16987 2/1/1 CNAME
      c.microsoft.akadns.net., A SA00 (125)16:28:44.568429 IP 172.21.20.20.2586
      > SA00.domain:  8026+ A? stats.update.microsoft.com. (44)
16:28:44.569140 IP SA00.domain > 172.21.20.20.2586:  8026 2/7/7 CNAME
      statsupdate.microsoft.com.nsatc.net., A 207.46.253.219 (354)



16:29:52.980950 IP 172.21.20.20.2586 > SA00.domain:  32089+ A?
      windowsupdate.microsoft.com. (45)
16:29:52.982836 IP SA00.domain > 172.21.20.20.2586:  32089 2/7/7 CNAME
      windowsupdate.microsoft.nsatc.net., A 207.46.225.221 (353)
16:29:53.792848 IP 172.21.20.20.2586 > SA00.domain:  15449+ A?
      update.microsoft.com. (38)
16:29:53.793619 IP SA00.domain > 172.21.20.20.2586:  15449 4/7/7 CNAME
      update.microsoft.com.nsatc.net., A 65.55.192.93, A 207.46.199.93, A
      207.46.211.126 (375)
16:29:56.514486 IP 172.21.20.20.2586 > SA00.domain:  64856+ A?
      download.windowsupdate.com. (44)
16:29:56.554654 IP SA00.domain > 172.21.20.20.2586:  64856 4/1/1 CNAME
      main.dl.wu.akadns.net., CNAME dom.dl.wu.akadns.net., CNAME
      dl.wu.ms.edgesuite.net., A SA00 (186)
```

```
16:29:56.590312 IP 172.21.20.20.2586 > SA00.domain:  3934+ A?
      download.microsoft.com. (40)
16:29:56.715218 IP SA00.domain > 172.21.20.20.2586:  3934 4/1/1 CNAME
      main.dl.ms.akadns.net., CNAME dom.dl.ms.akadns.net., CNAME dl.ms.d4p.net.,
      A SA00 (173)
16:29:57.402083 IP 172.21.20.20.2586 > SA00.domain:  25181+ A? c.microsoft.com.
      (33)
16:29:57.403740 IP SA00.domain > 172.21.20.20.2586:  25181 2/1/1 CNAME
      c.microsoft.akadns.net., A 64.4.52.124 (129)
16:29:57.594467 IP 172.21.20.20.2586 > SA00.domain:  39004+ A?
      stats.update.microsoft.com. (44)
16:29:57.594970 IP SA00.domain > 172.21.20.20.2586:  39004 2/7/7 CNAME
      statsupdate.microsoft.com.nsatc.net., A 207.46.253.219 (354)

16:36:33.024729 IP 172.21.20.20.1045 > SA00.domain:  1716+ A?
      update.microsoft.com. (38)
16:36:33.137830 IP SA00.domain > 172.21.20.20.1045:  1716 4/7/7 CNAME
      update.microsoft.com.nsatc.net., A 65.55.192.61, A 207.46.199.93, A
      207.46.209.124 (375)
16:36:33.138046 IP SA00.domain > 172.21.20.20.1045:  1716 4/7/7 CNAME
      update.microsoft.com.nsatc.net., A 65.55.192.61, A 207.46.199.93, A
      207.46.209.124 (375)
16:36:33.138257 IP SA00.domain > 172.21.20.20.1045:  1716 4/7/7 CNAME
      update.microsoft.com.nsatc.net., A 65.55.192.61, A 207.46.199.93, A
      207.46.209.124 (375)
16:36:36.293170 IP 172.21.20.20.1045 > SA00.domain:  35771+ A?
      download.microsoft.com. (40)
16:36:36.784849 IP SA00.domain > 172.21.20.20.1045:  35771 7/1/1 CNAME
      main.dl.ms.akadns.net., CNAME dom.dl.ms.akadns.net., CNAME dl.ms.d4p.net.,
      CNAME dl.ms.georedirector.akadns.net., CNAME a767.ms.akamai.net., CNAME
      a767.ms.akamai.net.af838acf.1.cn.akamaitech.net., A SA00 (294)
16:37:21.172239 IP 172.21.20.20.1045 > SA00.domain:  16058+ A?
      windowsupdate.microsoft.com. (45)
16:37:21.173980 IP SA00.domain > 172.21.20.20.1045:  16058 2/7/7 CNAME
      windowsupdate.microsoft.nsatc.net., A 207.46.18.94 (353)
16:37:22.010491 IP 172.21.20.20.1045 > SA00.domain:  49850+ A?
      update.microsoft.com. (38)
16:37:22.011249 IP SA00.domain > 172.21.20.20.1045:  49850 4/7/7 CNAME
      update.microsoft.com.nsatc.net., A 207.46.209.124, A 65.55.192.61, A
      207.46.199.93 (375)
16:37:28.239306 IP 172.21.20.20.1045 > SA00.domain:  28344+ A?
      download.windowsupdate.com. (44)
16:37:29.242338 IP 172.21.20.20.1045 > SA00.domain:  28344+ A?
      download.windowsupdate.com. (44)
16:37:30.232002 IP 172.21.20.20.1045 > SA00.domain:  28344+ A?
      download.windowsupdate.com. (44)
16:37:32.234442 IP 172.21.20.20.1045 > SA00.domain:  28344+ A?
      download.windowsupdate.com. (44)
16:37:36.241194 IP 172.21.20.20.1045 > SA00.domain:  28344+ A?
      download.windowsupdate.com. (44)
16:37:40.332379 IP SA00.domain > 172.21.20.20.1045:  28344 6/1/1 CNAME
      main.dl.wu.akadns.net., CNAME dom.dl.wu.akadns.net., CNAME
      dl.wu.ms.edgesuite.net., CNAME a258.g.akamai.net., A 89.149.169.57, A
      89.149.169.66 (234)
16:37:40.332500 IP SA00.domain > 172.21.20.20.1045:  28344 6/1/1 CNAME
      main.dl.wu.akadns.net., CNAME dom.dl.wu.akadns.net., CNAME
      dl.wu.ms.edgesuite.net., CNAME a258.g.akamai.net., A 89.149.169.57, A
      89.149.169.66 (234)
```

```
16:37:40.332613 IP SA00.domain > 172.21.20.20.1045:  28344 6/1/1 CNAME
      main.dl.wu.akadns.net., CNAME dom.dl.wu.akadns.net., CNAME
      dl.wu.ms.edgesuite.net., CNAME a258.g.akamai.net., A 89.149.169.57, A
      89.149.169.66 (234)
16:37:40.332723 IP SA00.domain > 172.21.20.20.1045:  28344 6/1/1 CNAME
      main.dl.wu.akadns.net., CNAME dom.dl.wu.akadns.net., CNAME
      dl.wu.ms.edgesuite.net., CNAME a258.g.akamai.net., A 89.149.169.57, A
      89.149.169.66 (234)
16:37:40.332837 IP SA00.domain > 172.21.20.20.1045:  28344 6/1/1 CNAME
      main.dl.wu.akadns.net., CNAME dom.dl.wu.akadns.net., CNAME
      dl.wu.ms.edgesuite.net., CNAME a258.g.akamai.net., A 89.149.169.57, A
      89.149.169.66 (234)
16:37:41.221871 IP 172.21.20.20.1045 > SA00.domain:  19903+ A? c.microsoft.com.
      (33)
16:37:41.222415 IP SA00.domain > 172.21.20.20.1045:  19903 2/1/1 CNAME
      c.microsoft.akadns.net., A 64.4.52.124 (129)
16:37:58.871182 IP 172.21.20.20.1045 > SA00.domain:  1471+ A?
      download.windowsupdate.com. (44)
16:37:58.872948 IP SA00.domain > 172.21.20.20.1045:  1471 6/1/1 CNAME
      main.dl.wu.akadns.net., CNAME dom.dl.wu.akadns.net., CNAME
      dl.wu.ms.edgesuite.net., CNAME a258.g.akamai.net., A 89.149.169.66, A
      89.149.169.57 (234)
```

Always Granting Access to an Endpoint

To always grant access to a endpoint without testing:

NAC 800 Home window>>System configuration>>Exceptions

The following figure shows the **Exceptions** window.

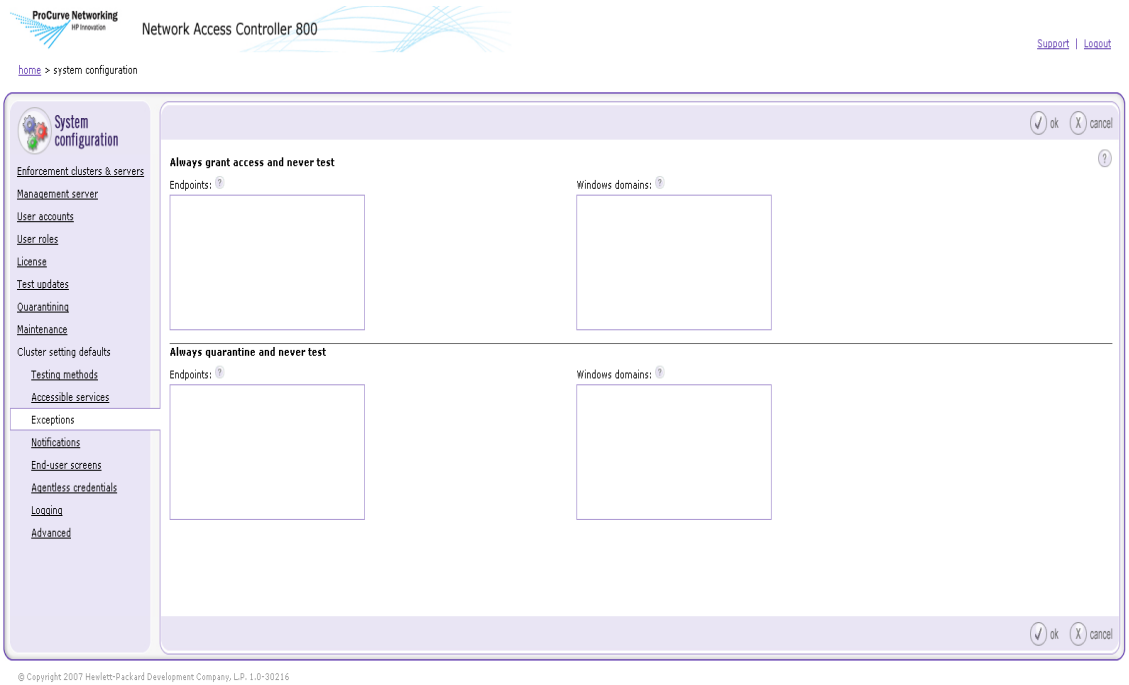


Figure 7-4. Exceptions Window

1. In the **Always grant access and never test** area:
   a. In the **Endpoints** area, enter one or more MAC addresses, IP addresses, or NetBIOS names separated by carriage returns.
   b. In the **Windows domains** area, enter one or more domain names separated by carriage returns.
2. Click **ok**.

CAUTION: If you enter the same endpoint for both options in the Endpoint testing exceptions area, the Allow access without testing option is used.

CAUTION: Please read "Untestable Endpoints and DHCP Mode" on page 7-18 so that you fully understand the ramifications of allowing untested endpoints on your network.

Always Quarantining an Endpoint

To always quarantine a an endpoint without testing (cluster default):

NAC 800 Home window>>System configuration>>Exceptions

1. In the **Always quarantine and never test** area:
   a. In the **Endpoints** area, enter one or more MAC addresses, IP addresses, or NetBIOS names separated by carriage returns.
   b. In the **Windows domains** area, enter one or more domain names separated by carriage returns.
2. Click **ok**.

CAUTION:

If you enter the same endpoint for both options in the Endpoint testing exceptions area, the Allow access without testing option is used.

New Users

The process NAC 800 follows for allowing end-users to connect is:

- Inline mode – An IP address is assigned to the endpoint outside of NAC 800. When the end-user attempts to connect to the network, NAC 800 either blocks access or allows access by adding the endpoint IP address to the internal firewall.
- DHCP mode – New end-users boot their computers. The boot process looks for an IP address and, because they are new end-users and no information is known about the endpoints, a temporary quarantined IP address is assigned. The end-users log in on the Windows login screen. The end-users start IE and NAC 800 attempts to test the endpoint. The endpoints either retain the quarantined IP address, or are assigned a non-quarantined network IP address based on the testing result.
- 802.1X mode – An endpoint attempts to connect to the network. The end-user's identity is verified via an authentication server. If the endpoint is not authenticated, it is quarantined (allowed access to a limited VLAN). If the endpoint is authenticated, it is tested by NAC 800. If the endpoint fails the NAC 800 testing, it is quarantined (allowed access to a limited VLAN). If the endpoint passes the NAC 800 testing, it is allowed access to the network (VLAN).

Shared Resources

If the end-users typically make connections to shared services and endpoints during the boot process, these shares are unable to connect while the endpoint has the quarantined IP address, unless the services and endpoints are listed in the Accessible services and endpoints area (see “Accessible Services” on page 3-98). Once the endpoints are assigned a non-quarantined IP address, the users can gain access to the shares by logging out of Windows and logging back into Windows. Rebooting the endpoints also works, but is not necessary.

Untestable Endpoints and DHCP Mode

If you have an endpoint that does not have a supported operating system, you can allow access or quarantine the endpoint. The current supported operating systems are listed in “Endpoints Supported” on page 5-3.

If you allow an untested endpoint to have access, there are several important items to keep in mind.

The IP address granted by your DHCP server has a lease expiration period that cannot be affected by the NAC 800 server. Once an untested endpoint has been allowed access and assigned a non-quarantined IP address by your DHCP server, that endpoint has continual access through that IP address until the IP address lease expires. For example, you are not be able to quarantine that endpoint (or affect any other action on that endpoint) with NAC 800 until the lease expires. It is not unusual for system administrators to set a lease expiration time of three or more days.

NOTE: The access status column on the Endpoint activity window shows unable to quarantine, and the action cannot complete until the IP address lease expires.

TIP: It is strongly recommended that if you are going to allow untested endpoints on your network, you set extremely short lease times (use hours rather than days) on your DHCP server.

This process results in the following condition for an untested endpoint:

When new end-users log in for the first time, are tested, and are allowed access, there is up to a three-minute delay between the time the NAC 800 server determines that they are allowed access and the point at which they are actually allowed access, potentially causing concern to the end-user. This uncertainty is due to the three-minute lease on the temporary quarantined IP address assigned during the initial login process. Once the lease expires (in at most, three minutes), a new IP address (the non-quarantined IP address) can be assigned and access is actually granted.

To define access settings for non-supported operating systems, see “Defining Non-supported OS Access Settings” on page 6-15.

8

High Availability and Load Balancing

Chapter Contents

High Availability 8-2
Load Balancing 8-6

High Availability

High availability occurs when one or more Enforcement servers takes over for an Enforcement server that has become unavailable in a multiple-server installation.

Once an ES becomes unavailable, the other ESs take over enforcement from the ES that is now unavailable. All ESs participate in enforcement. The MS provides notification in the console at the top of the **Home** window. For example, if an ES is unavailable, the notification indicates that at the top of the **Home** window.

When NAC 800 is installed inline in a multiple-server configuration (figure 8-1), the multiple Enforcement servers (ESs) form a network loop (an undesired condition). The Spanning Tree Protocol (STP) detects the loop and closes one of the offending ports on the switch based on the switch configuration. If an

ES becomes unavailable, the switch reconnects so that there is always a path from the VPN to an ES. All of the ES firewalls continuously stay in sync with each other.

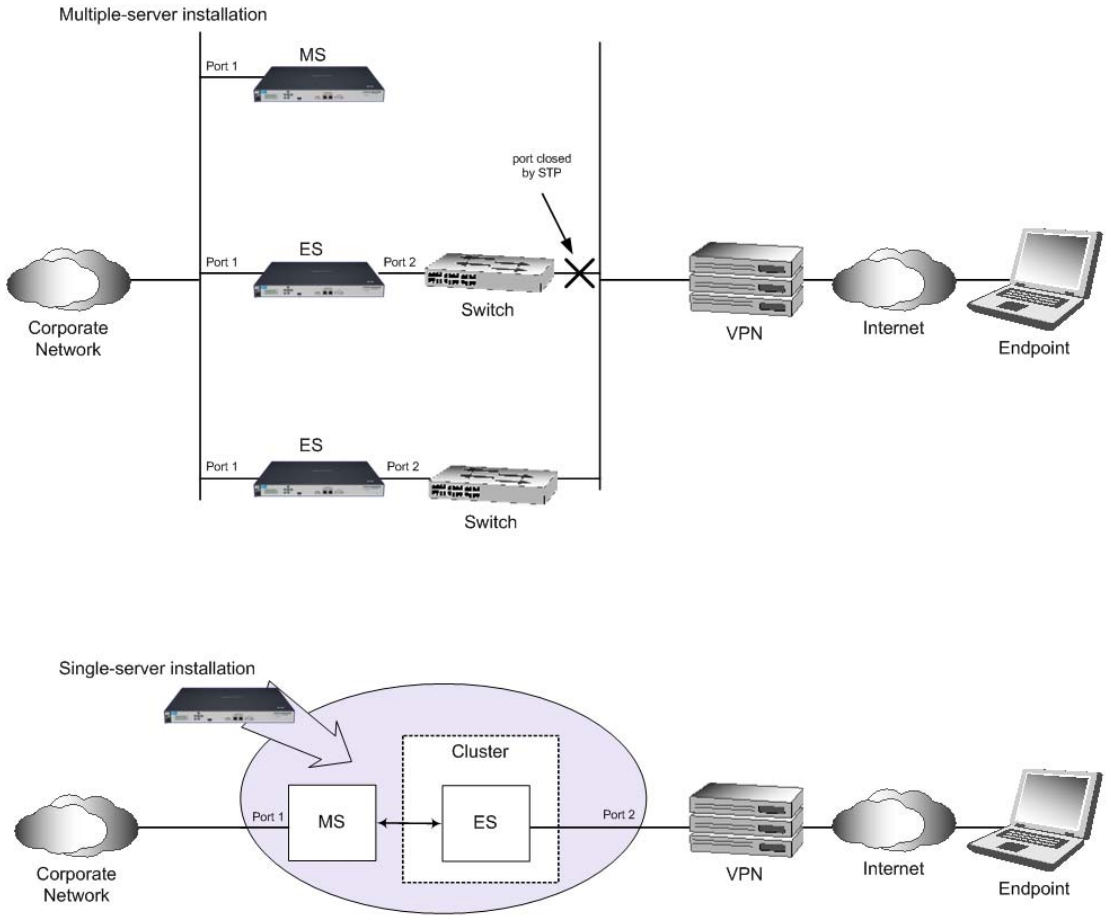


Figure 8-1. Inline Installations

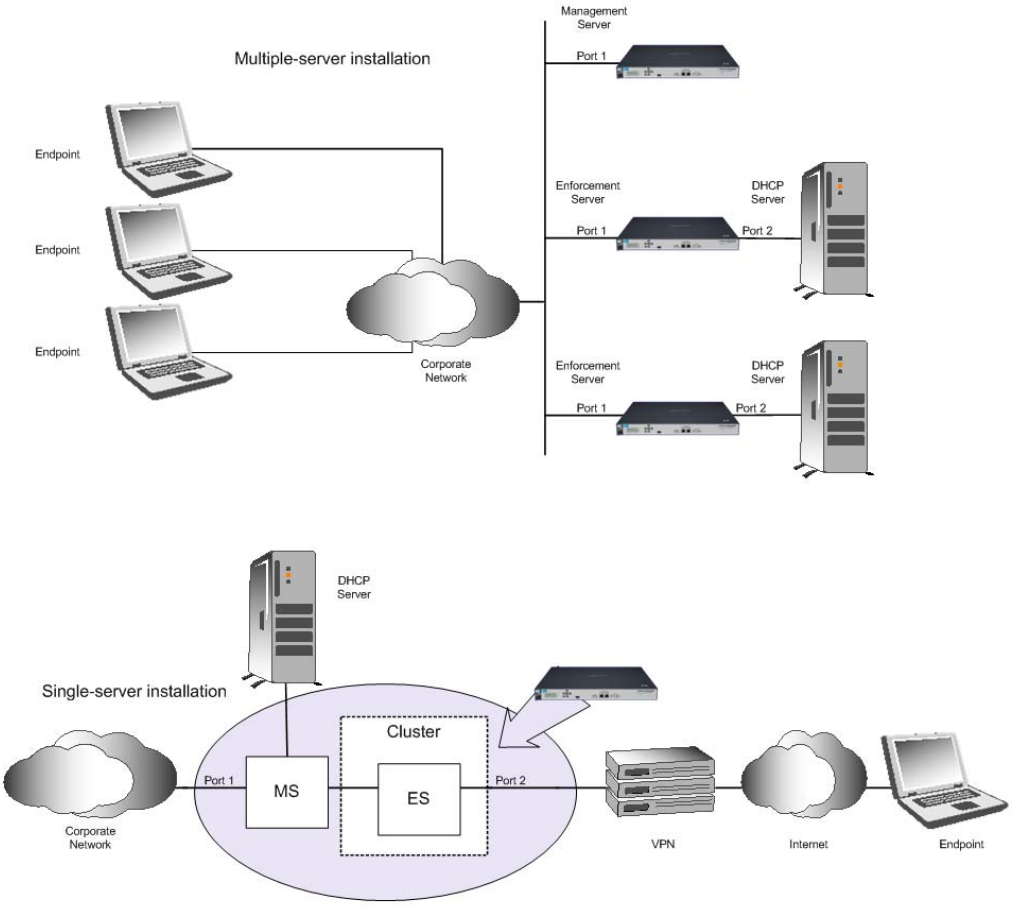


Figure 8-2. DHCP Installation

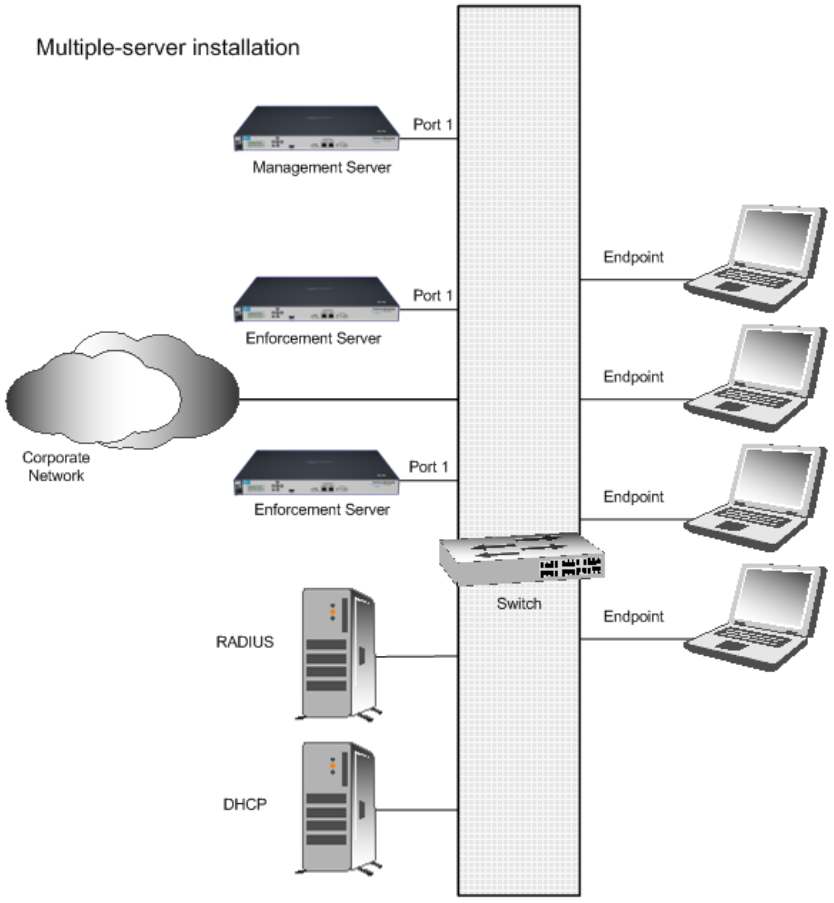


Figure 8-3. 802.1X Installation

Load Balancing

Load balancing distributes the testing of endpoints across all NAC 800 Enforcement servers in a cluster. NAC 800 uses a hashing algorithm based on MAC or IP addresses to divide the endpoints between the Enforcement servers.

If the MAC address is unavailable (untestable endpoint) the IP address is used to determine which ES should test an endpoint. If an ES detects an endpoint for which it is not responsible, it notifies the correct ES of the endpoint and that ES takes over testing.

If an ES fails, any services that are *protected* by that ES may become inaccessible, depending on the nature of the ES failure. However, the redundant services that are *protected* by the other ESs are still available.

TIP: Protected services are services that are running on any servers that sit on the eth1 side of the failed ES, such as AD, DNS, DHCP, NTP, file server, print server, and so on.

9

Inline Quarantine Method

Chapter Contents

Inline 9-2

Inline

Inline is the most basic NAC 800 installation. When deploying NAC 800 inline, NAC 800 monitors and enforces all endpoint traffic.

When NAC 800 is installed in a single-server installation, NAC 800 becomes a Layer 2 bridge that requires no changes to the network configuration settings. When NAC 800 is installed in a multiple-server installation, you may have to configure the switch that connects the NAC 800 Enforcement servers to use Spanning Tree Protocol (STP) if STP is not already configured.

NAC 800 allows endpoints to access the network or blocks endpoints from accessing the network based on their Internet Protocol (IP) address with a built-in firewall (iptables).

When NAC 800 is installed inline in a multiple-server configuration (figure 9-1), the multiple Enforcement servers (ESs) form a network loop (an undesired condition). The Spanning Tree Protocol (STP) detects the loop and closes one of the offending ports on the switch based on the switch configuration. If an

ES becomes unavailable, the switch reconnects so that there is always a path from the VPN to an ES. All of the ES firewalls continuously stay in sync with each other.

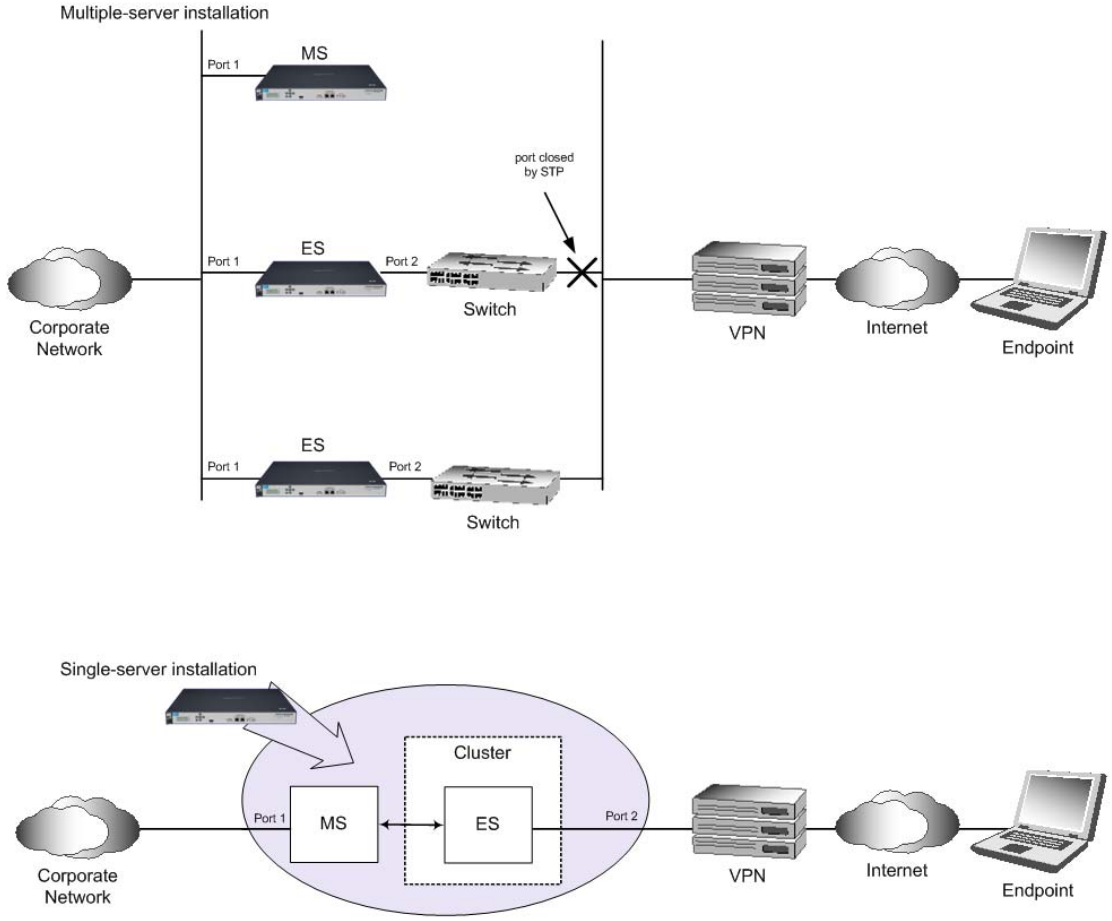


Figure 9-1. Inline Installations

TIP: You can install NAC 800 at any "choke point" in your network; a VPN is not required.

(This page intentionally left blank.)

10

DHCP Quarantine Method

Chapter Contents

Overview 10-2
Configuring NAC 800 for DHCP 10-4
Setting Up a Quarantine Area 10-4
Router Configuration 10-4

Overview

When configured with a Dynamic Host Configuration Protocol (DHCP) quarantine area, all endpoints requesting a DHCP IP address are issued a temporary address on a quarantine subnetwork. Once the endpoint is allowed access, the IP address is renewed and the main DHCP server assigns an address to the main LAN.

With a multiple subnetwork or VLAN network, one quarantine area must be configured for each subnetwork.

Quarantine areas are defined on a per-cluster basis and pushed down to all Enforcement servers joined to that cluster.

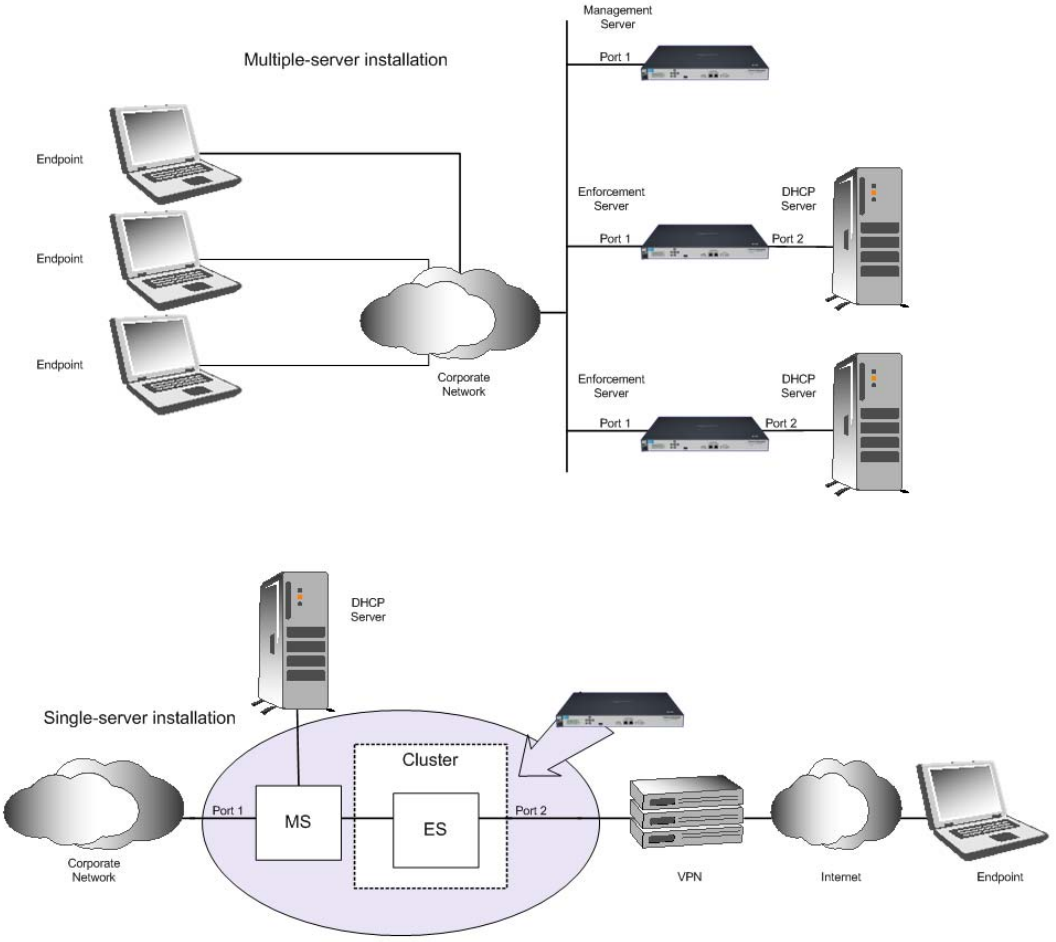


Figure 10-1. DHCP Installation

Configuring NAC 800 for DHCP

The primary configuration required for using NAC 800 and DHCP is setting up the quarantine area (see "Setting Up a Quarantine Area" on page 10-4). You should also review the following topics related to quarantining endpoints:

- Endpoint quarantine precedence (see "Endpoint Quarantine Precedence" on page 7-2).
- Untested endpoints (see "Untestable Endpoints and DHCP Mode" on page 7-18).
- Unsupported operating systems (see "Defining Non-supported OS Access Settings" on page 6-15).
- Endpoint testing exceptions (see "Always Granting Access to an Endpoint" on page 7-13 and "Always Quarantining an Endpoint" on page 7-15).
- Action to take for failed tests (see "Selecting Action Taken" on page 6-15)
- DHCP quarantine options:
  - Router Access Control List (ACL) settings (see "Configuring the Router ACLs" on page 10-5).
  - Static routes assigned to the endpoint (see "Adding a DHCP Quarantine Area" on page 3-87)

Setting Up a Quarantine Area

Set up a restricted area of your network that users can access when you do not want to allow full access to the network. See "Quarantining" on page 3-49 for instructions.

Router Configuration

If you do not elect to enforce using static routes on the endpoint ("Quarantining" on page 3-49), you will need to configure router ACLs.

This option restricts the network access of non-compliant endpoints by assigning DHCP settings on a quarantined network. The network, gateway, and ACLs restricting traffic must be configured on your router, which is accomplished by multinetting or adding a virtual interface to the router that acts as the quarantine gateway IP address. The quarantine area DHCP settings must reflect this configuration on your router.

Configuring the Router ACLs

In order to sufficiently restrict access to and from the quarantine area, you must configure your router Access Control Lists (ACLs) as follows:

- Allow traffic to and from the NAC 800 server and the quarantined network.
- If you want to allow access to other endpoints outside of the quarantine area (for example a Software Update Service (SUS) server), allow access to the server and port to and from the quarantined network.
- All other traffic should be denied both *to* and *from* the quarantined network.

TIP: Restrict access to and from the quarantined network at the switch level as well.

Configuring Windows Update Service for XP SP2

If you plan to use Endpoint Routing Enforcement, note that most endpoints running Windows XP Service Pack 2 cannot run Windows Update successfully from within quarantine, because of a WinHTTP bug that as of this writing has not been fixed (see http://support.microsoft.com/kb/919477/ for more details.) Endpoints not in quarantine are not affected.

The problem occurs because the Windows Update (WU) client software uses WinHTTP to connect to Microsoft's download sites; Internet Explorer connects to windowsupdate.microsoft.com; however, an error is displayed once the user clicks on the **Express** or **Custom** download buttons that invoke the WU client software.

Short of a Microsoft fix, the only way to update XP SP2 endpoints in quarantine is to deploy a local update server (such as Microsoft's free Windows Server Update Services, WSUS -- see http://www.microsoft.com/technet/windowsserver/wsus/default.mspx) and make sure that this server is listed in **Accessible Services and Devices** (“Accessible Services” on page 3-98).

(This page intentionally left blank.)

11

802.1X Quarantine Method

Chapter Contents

About 802.1X 11-2
NAC 800 and 802.1X 11-4
Setting Up the 802.1X Components 11-7
- Setting up the RADIUS Server 11-7
- Enabling NAC 800 for 802.1X 11-43
- Setting Up the Supplicant 11-44
- Setting Up the Authenticator 11-47

About 802.1X

802.1X is a port-based authentication protocol that can dynamically vary encryption keys, and has three components as follows:

- Supplicant – The client; the endpoint that wants to access the network.
- Authenticator– The access point, such as a switch, that prevents access when authentication fails. The authenticator can be simple and dumb.
- Authentication server – The server that authenticates the user credentials; usually a Remote Authentication Dial-In User Service (RADIUS) server.

802.1X is an authentication framework that sends Extensible Authentication Protocol (EAP) messages packaged in Ethernet frames over LANs (EAPOL). This method provides a savings in overhead resources because it does not use all of the resources the typical Point-to-Point protocol requires.

EAP supports multiple authentication methods such as:

- Kerberos – An authentication system that uses an encrypted ticket to authenticate users.
- One-time passwords – An authentication system that uses a set of rotating passwords, each of which is used for only one login session.
- Certificates – A method for identifying a user that links a public key to the user's or company's identity, allowing them to send digitally signed electronic messages.
- Tokens – A credit-card or key-fob sized authentication endpoint that displays a number that is synchronized with the authentication server. The number changes over time, and the user is required to enter the current number as part of the authentication process.
- Public key authentication – In an asymmetric encryption system, two keys are required; a public key and a private key. Either key can encrypt and decrypt messages, but cannot encrypt and decrypt the same message; that is, if the public key encrypts a message, the private key must decrypt the message.

The typical 802.1X connections are shown in Figure 11-1 on page 11-3; The typical communication flow is as follows:

1. A Client (supplicant) requests access from the access point (AP) (authenticator).

2. The AP (authenticator) opens a port for EAP messages, and blocks all others.
3. The AP (authenticator) requests the client's (supplicant's) identity.
4. The Client (supplicant) sends its identity.
5. The AP (authenticator) passes the identity on to the authentication server.
6. The authentication server performs the authentication and returns an accept or reject message to the AP (authenticator).
7. The AP (authenticator) allows or blocks the client's (supplicant's) access to the network by controlling which ports are open or closed.

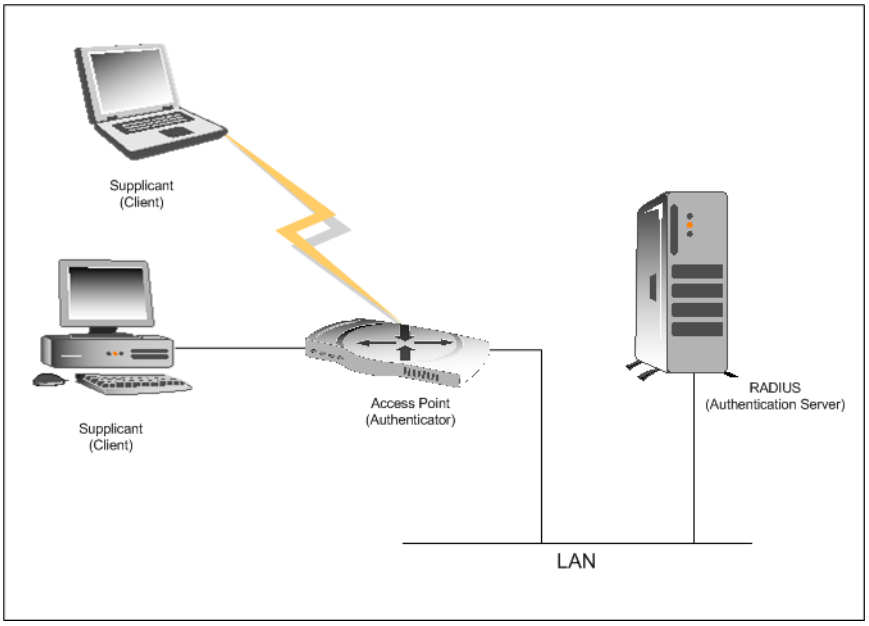


Figure 11-1. 802.1X Components

NAC 800 and 802.1X

When configured as 802.1X-enabled, NAC 800 can be installed with three different configurations depending on your network environment:

- Microsoft IAS and NAC 800 IAS Plug-in

  With this method, the switch is configured with the IAS server IP address as the RADIUS server host. When the switch performs the RADIUS authentication, IAS authenticates the user. If successful, IAS then calls the NAC 800 plug-in, which asks NAC 800 for the health status of the endpoint. You can configure up to six NAC 800 server URLs. The plug-in reads the list of servers over and over (iterates) attempting to connect to one of them. Once a connection is made, the NAC 800 plug-in uses that server URL until it is no longer available, at which point it iterates over the list of servers again. If necessary, the NAC 800 plug-in overwrites the RADIUS attributes to specify the VLAN to place the endpoint into. IAS then returns the results to the switch.

- Proxying RADIUS requests to an existing RADIUS server

  With this method, the switch is configured with the NAC 800 IP address as the RADIUS server host. When the switch performs the RADIUS authentication against the NAC 800 server, NAC 800 proxies the request to another RADIUS server. As long as that server supports the appropriate authentication methods used by the client it should allow and authenticate the proxied requests. On successful authentication, when the end RADIUS server returns the proxied request NAC 800 overrides the RADIUS attributes which specify to the switch which VLAN to place the endpoint in if necessary. NAC 800 then returns the authentication results to the switch.

- Using the built-in NAC 800 RADIUS server

  With this method, all authentication takes place on the NAC 800 server. The switch is configured with the NAC 800 IP address as the RADIUS server host. NAC 800 performs the authentication based on the FreeRadius configuration, inserts RADIUS attributes specifying into which VLAN to place the endpoint, and returns the result to the switch.

When NAC 800 is used in an 802.1X network, the configuration is as shown in figure 11-2, and the communication flow is shown in Figure 11-3 on page 11-6.

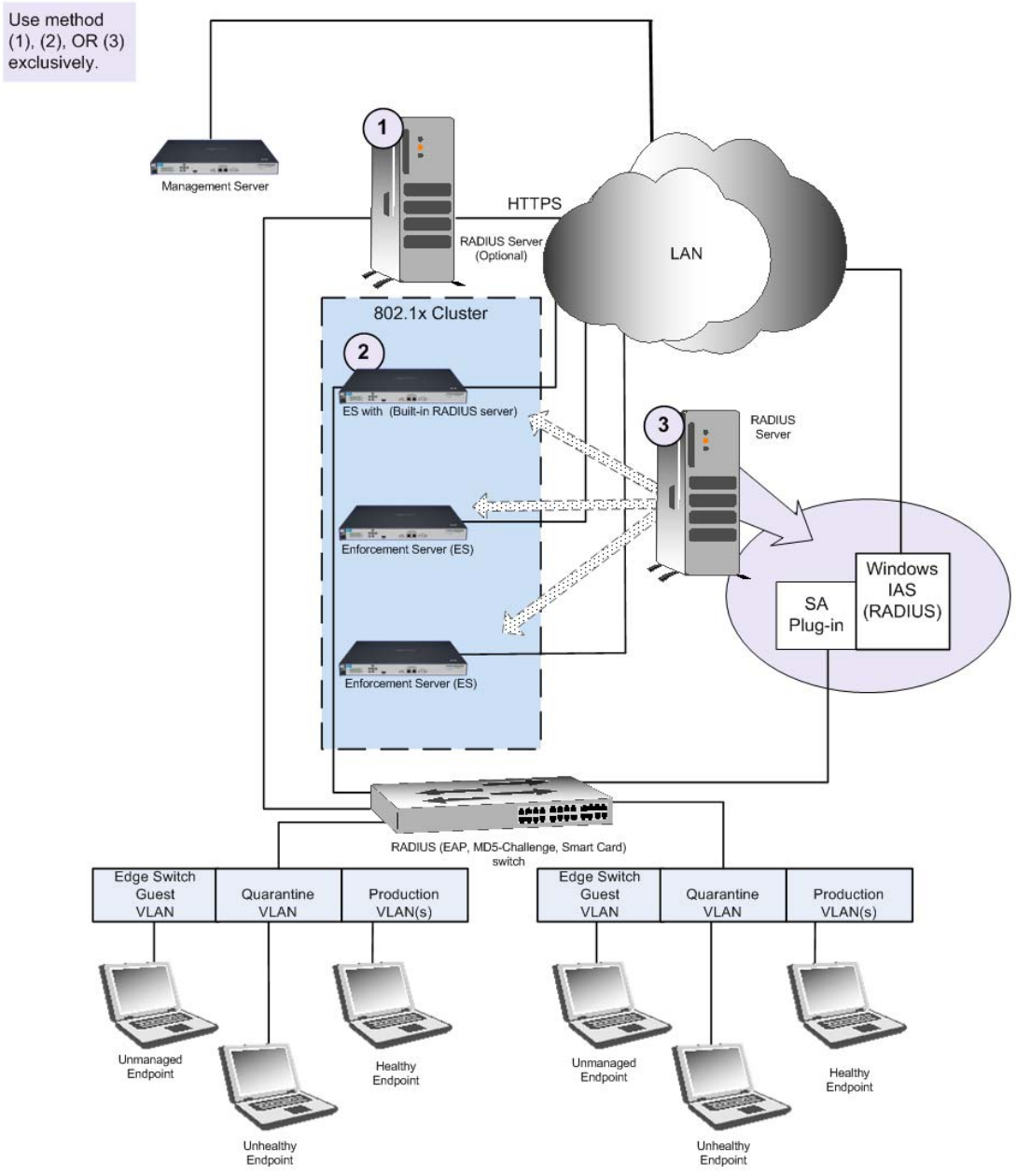


Figure 11-2. NAC 800 802.1X Enforcement

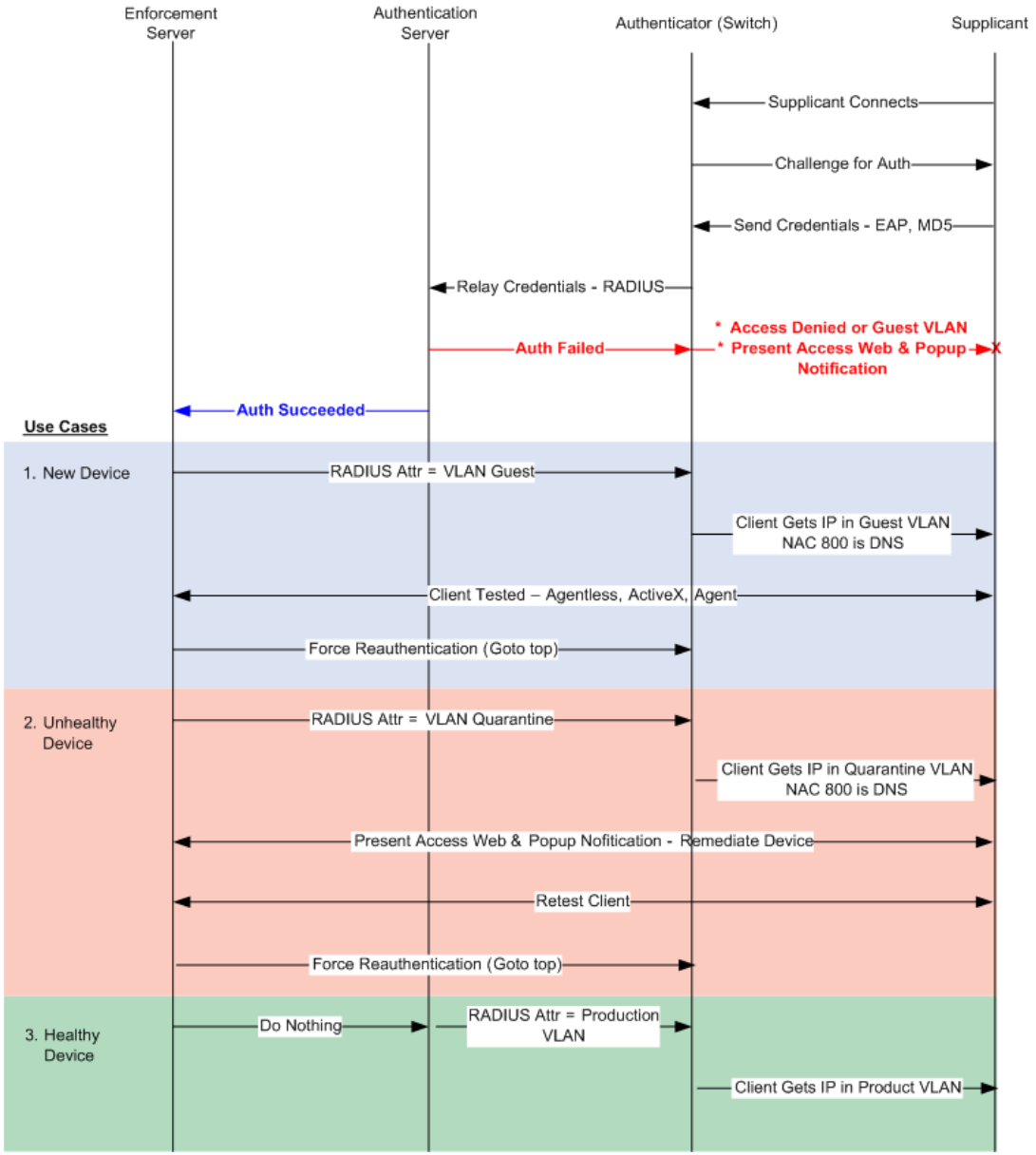


Figure 11-3. 802.1X Communications

Setting Up the 802.1X Components

In order to use NAC 800 in an 802.1X environment, ProCurve recommends configuring your environment first, then installing and configuring NAC 800.

This section provides instructions for the following:

- "Setting up the RADIUS Server" on page 11-7
- "Enabling NAC 800 for 802.1X" on page 11-43
- "Setting Up the Supplicant" on page 11-44
- "Setting Up the Authenticator" on page 11-47

Setting up the RADIUS Server

Switches support 802.1X authentication by authenticating against a RADIUS server. The NAC 800 802.1X solution must be integrated with the RADIUS authentication to "intervene" in the authentication process, test endpoints, and assign them to the appropriate VLAN. NAC 800 can be deployed and integrated with RADIUS in the following three ways:

- Install the NAC 800 Plug-in to the Microsoft® IAS RADIUS server (see "This section provides instructions for how to install the Microsoft IAS to the NAC 800 IAS plug-in." on page 11-7).
- Proxy requests from the built-in NAC 800 RADIUS server to any other RADIUS server (see "Proxying RADIUS Requests to an Existing RADIUS Server Using the Built-in NAC 800 RADIUS Server" on page 11-37).
- Use the built-in NAC 800 RADIUS server for authentication (see "Enabling NAC 800 for 802.1X" on page 11-43).

Any of these solutions can be customized to work with your existing LDAP or Active Directory user databases. This section provides instructions of configuring these three options.

Using the NAC 800 IAS Plug-in to the Microsoft IAS RADIUS Server

This section provides instructions for how to install the Microsoft IAS to the NAC 800 IAS plug-in.

TIP: For an explanation of how the components communicate, see "NAC 800 and 802.1X" on page 11-4.

Microsoft® Windows Server™ 2003 Internet Authentication Service (IAS) is Microsoft's implementation of a Remote Authentication Dial-In User Service (RADIUS) server. This section provides instructions on configuring this server to use with NAC 800.

For details on the Windows Server 2003 IAS, refer to the following link:

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/ias.mspx

In addition to installing the Windows Server 2003 software, you also need to have a database of users for authentication purposes. The Windows IAS implementation of RADIUS can use the following:

- Active Directory (*recommended*)
- A Windows NT domain
- The local Security Accounts Manager (SAM)

To add IAS to the Windows Server 2003 installation:

Windows desktop

1. Select **Start>>Settings>>Control Panel>>Add or remove programs**.
2. In the left column, click **Add/Remove Windows Components**. The **Windows Components Wizard** window appears, as shown in the following figure.

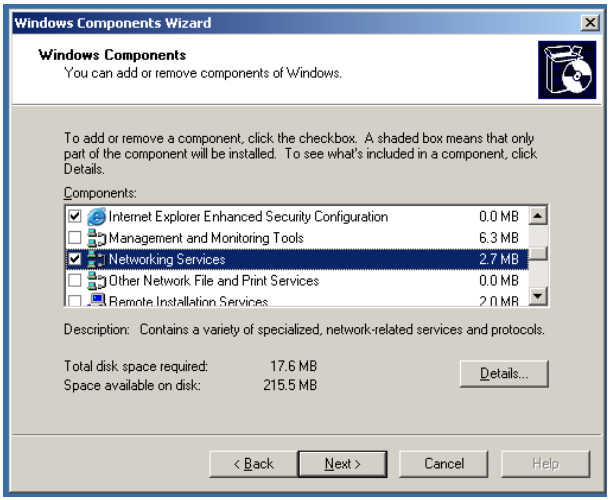

Windows Components Wizard
Windows Components
You can add or remove components of Windows.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Internet Explorer Enhanced Security Configuration 0.0 MB
Management and Monitoring Tools 6.3 MB
Networking Services 2.7 MB
Other Network File and Print Services 0.0 MB
Description: Contains a variety of specialized, network-related services and protocols.
Total disk space required: 17.6 MB
Space available on disk: 215.5 MB
Details...
< Back
Next >
Cancel
Help

Figure 11-4. Windows Components Wizard Window

3. Select the **Networking Services** check box.
4. Click **Details**. The **Networking Services** window appears, as shown in the following figure.

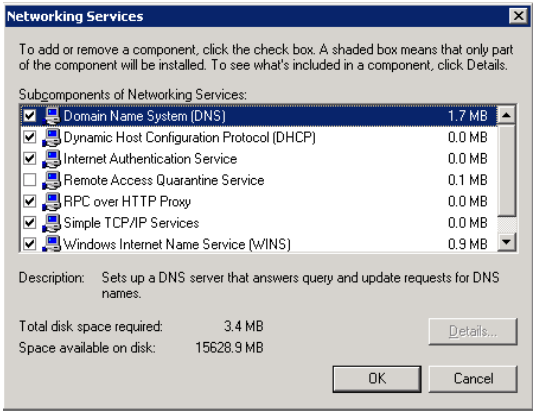

Networking Services
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Networking Services:
Domain Name System (DNS) 1.7 MB
Dynamic Host Configuration Protocol (DHCP) 0.0 MB
Internet Authentication Service 0.0 MB
Remote Access Quarantine Service 0.1 MB
RPC over HTTP Proxy 0.0 MB
Simple TCP/IP Services 0.0 MB
Windows Internet Name Service (WINS) 0.9 MB
Description: Sets up a DNS server that answers query and update requests for DNS names.
Total disk space required: 3.4 MB
Space available on disk: 15628.9 MB
Details...
OK
Cancel

Figure 11-5. Networking Services Window

5. Select the check box for **Internet Authentication Service** and any other Windows Internet Authentication Service (IAS) components you want to install.
6. Click **OK**.
7. Click **Next**.
8. Click **Finish**.
9. Install any IAS and 802.1X updates that are available.

   http://www.microsoft.com/downloads/search.aspx?displaylang=en

Configuring the Microsoft IAS RADIUS server

For an explanation of how the components communicate, see “NAC 800 and 802.1X” on page 11-4.

Now that you have the RADIUS server installed, you need to log into it and perform the configuration steps described in this section.

To configure the RADIUS server:

1. Log into the RADIUS server.
2. From the RADIUS server main window, select **Start>>Settings>>Control Panel>>Administrative Tools>>Internet Authentication Service.**
3. Configure IAS to use Active Directory:
   a. Right-click on **Internet Authentication Service (Local).**
   b. Select **Register Server in Active Directory (**figure 11-6).
   c. Click **OK** if a registration completed window appears.

4. Configure the RADIUS server parameters:

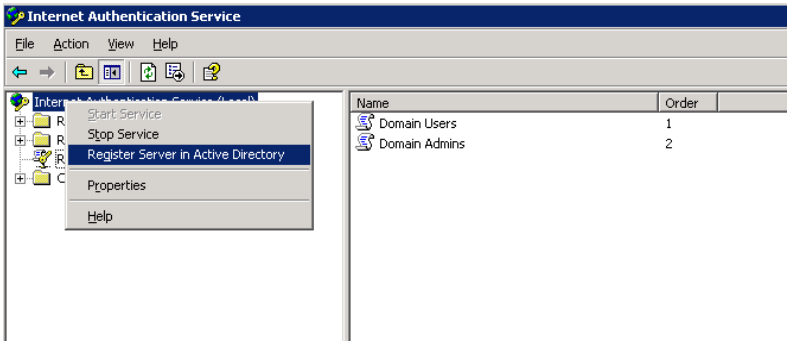


Figure 11-6. IAS, Register Server in Active Directory Window

a. Right-click on **Internet Authentication Service (local)**

b. Select **Properties (**figure 11-7). The **Properties** window appears (figure 11-8).

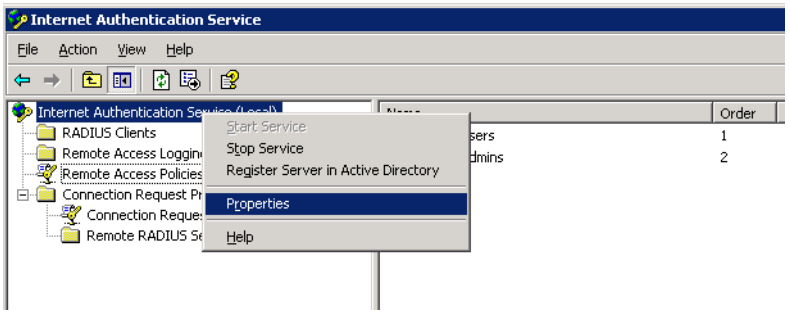


Figure 11-7. IAS, Properties Option

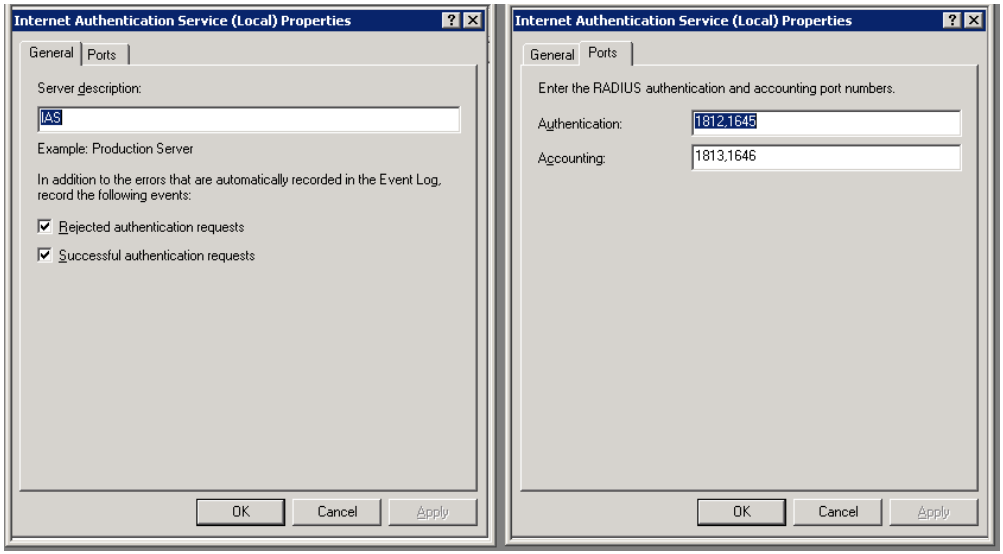


Figure 11-8. IAS, Properties Window

c. General tab –
   i. Enter a descriptive name in the **Server Description** text box. For example, `IAS`.
   ii. Select the **Rejected authentication requests** check box.
   iii. Select the **Successful authentication requests** check box.

d. Ports tab –
   i. Enter the authentication port number(s) in the **Authentication** text box. The authentication port (1812) is used to verify the user.
   ii. Enter the accounting port number(s) in the **Accounting** text box. The accounting port (1813) is used to track the user's network use.

e. Click **OK**.

5. Define the authenticators that use this RADIUS server for authentication.
   a. Right-click on **RADIUS Clients**.
   b. Select **New RADIUS Client**. The **New RADIUS Client** window appears:

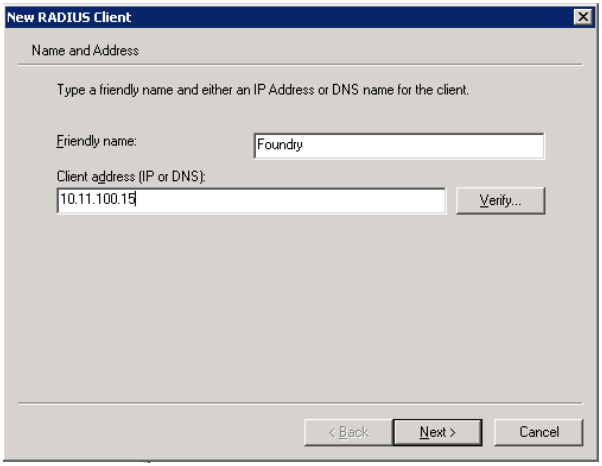


Figure 11-9. IAS, New Client, Name and Address Window

c. Enter a descriptive name for the **Frendly name**, such as `Foundry`.

d. Enter the IP address of the authenticator in the **Client address** text box.

TIP: Click Verify to test the connection.

e. Click **Next**.

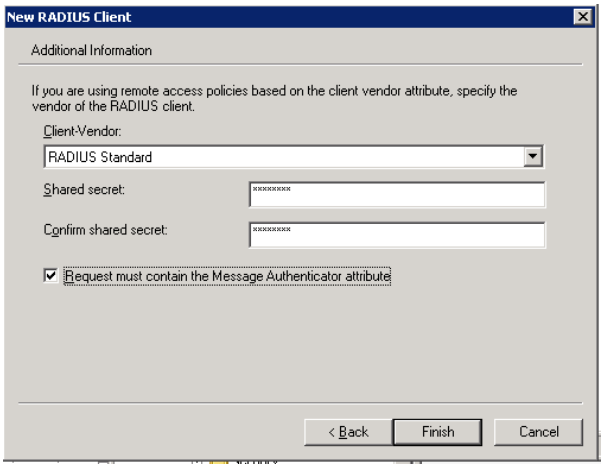

New RADIUS Client
Additional Information
If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client.
Client-Vendor:
RADIUS Standard
Shared secret:
Confirm shared secret:
Request must contain the Message Authenticator attribute
< Back
Finish
Cancel

Figure 11-10. IAS, New Client, Additional Information Window

f. Select **RADIUS Standard** from the **Client Vendor** drop-down list

g. Enter a password in the **Shared secret** text box. This password also needs to be entered when you configure the authenticator.

h. Re-enter the password in the **Confirm shared secret text** box.

i. Select the **Request must contain the Message Authenticator attribute** check box.

j. Click **Finish**.

6. Repeat step 5 for every authenticator in your system that uses this RADIUS server.

7. Create a Remote Access Policy:

   If you already have an 802.1X environment configured, you already have a Remote Access Policy defined; however, you can create as many as you need.

   a. Right-click on **Remote Access Policy.**

   b. Select **New Remote Access Policies**.

   c. Click **Next**. The **New Remote Access Policy Wizard** window appears:

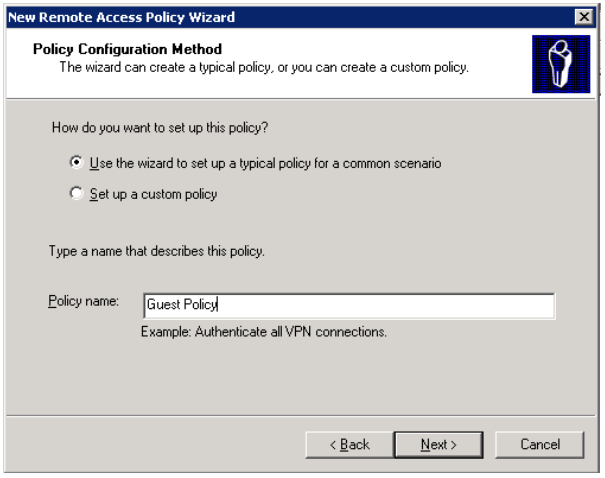

New Remote Access Policy Wizard
Policy Configuration Method
The wizard can create a typical policy, or you can create a custom policy.
How do you want to set up this policy?
Use the wizard to set up a typical policy for a common scenario
Set up a custom policy
Type a name that describes this policy.
Policy name:
Guest Policy
Example: Authenticate all VPN connections.
< Back
Next >
Cancel

Figure 11-11. IAS, New Remote Access Policy

d. Select the **Use the wizard** radio button.

e. Enter a meaningful name in the **Policy Name** text field.

f. Click **Next**.

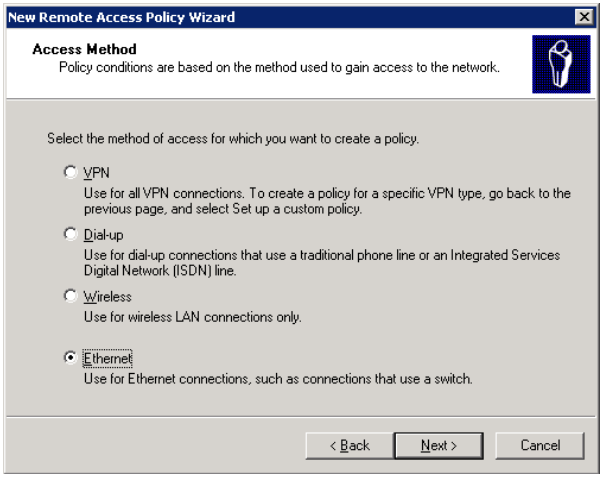

New Remote Access Policy Wizard
Access Method
Policy conditions are based on the method used to gain access to the network.
Select the method of access for which you want to create a policy.
VPN
Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.
Dial-up
Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.
Wireless
Use for wireless LAN connections only.
Ethernet
Use for Ethernet connections, such as connections that use a switch.
< Back
Next >
Cancel

Figure 11-12. IAS, Remote Access Policy, Access Method

g. Select the **Ethernet** radio button. (The Ethernet option will not work for authenticating wireless clients with this policy.)

h. Click **Next**.

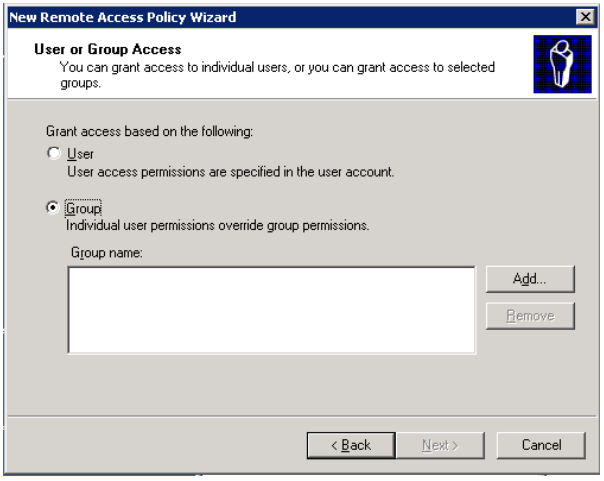

New Remote Access Policy Wizard
User or Group Access
You can grant access to individual users, or you can grant access to selected groups.
Grant access based on the following:
User
User access permissions are specified in the user account.
Group
Individual user permissions override group permissions.
Group name:
Add...
Remove
< Back
Next >
Cancel

Figure 11-13. IAS, Remote Access Policy, Group Access

i. You can configure your Access policy by user or group. This example uses the group method. Select the **Group** radio button.

j. Click **Add**. The **Select Groups** pop-up window appears:

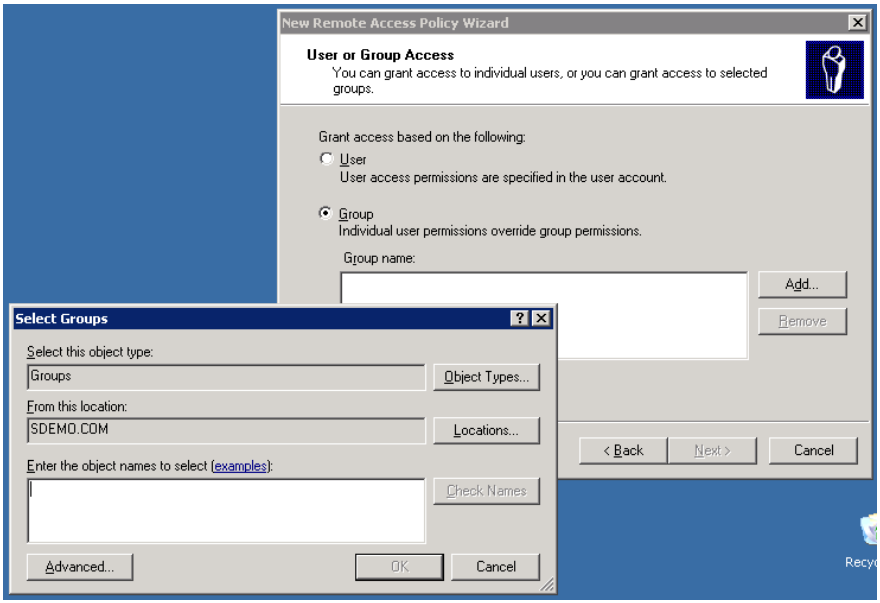


Figure 11-14. IAS, Remote Access Policy, Find Group

k. Click **Advanced**.

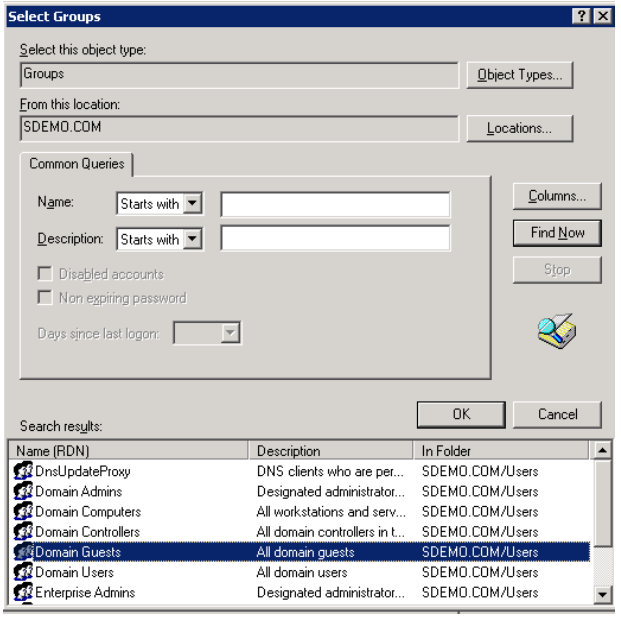


Figure 11-15. Remote Access Policy, Select Group

l. Click **Find Now** to populate the **Search Results** area.

m. Select **Domain Guests**.

n. Click **OK**.

o. Click **OK**.

p. Click **Next**.

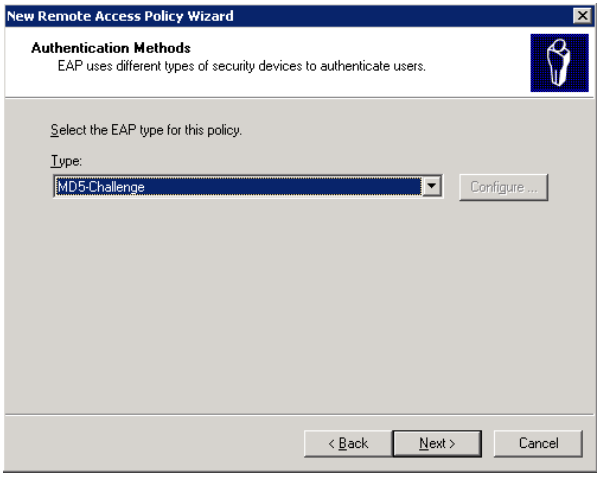


Figure 11-16. IAS, Remote Access Policy, Authentication Method

NOTE:

If you choose PEAP as your authentication mechanism in step q, see step 8 before completing step r and step s. Adding a certificate, if your server does not already have one, and configuring PEAP is explained in step 8.

q. Select the EAP type from the drop-down list.

   Important: The type selected here must match the type selected for the endpoint described in step 4, step b on page 11-45.

r. Click **Next**.

s. Click **Finish**.

8. The PEAP authentication method requires that a specific type of SSL certificate is available for use during authentication. These steps assume there is a Domain Certificate Authority (CA) is available to request a certificate.

   Click **Configure**.

   If you receive the error message shown in figure 11-7, complete these steps to request a certificate.

   These steps assume there is a Domain Certificate Authority (CA) available

to request a certificate. If there is not a CA available, the certificate needs to be imported manually.

To request a certificate from a Domain Certificate Authority:

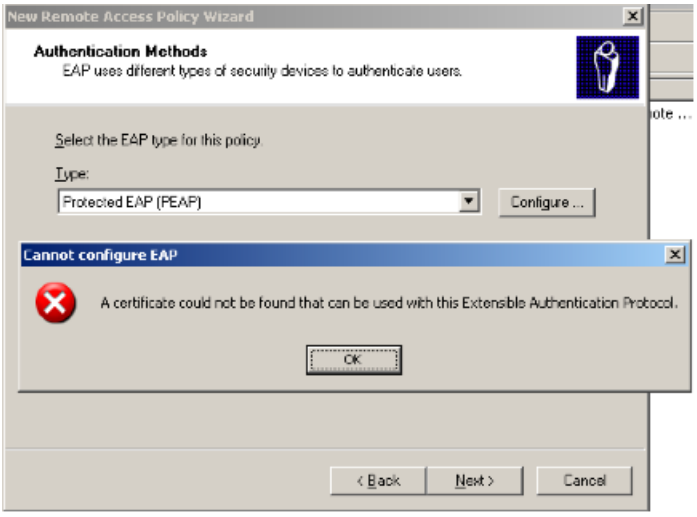

New Remote Access Policy Wizard
Authentication Methods
EAP uses different types of security devices to authenticate users.
Select the EAP type for this policy.
Type:
Protected EAP (PEAP)
Configure...
Cannot configure EAP
A certificate could not be found that can be used with this Extensible Authentication Protocol.
OK
< Back
Next >
Cancel

Figure 11-17. Error Message

a. Open the Microsoft management console by choosing **Start>>Run** and entering `mmc`.
b. Choose **File>>Add/Remove Snap-in**.
c. Click **Add**.
d. Choose the certificates snap-in and click **Add**.
e. Select **Computer account** and click **Next**.
f. Select **Local Computer** and click **Finish**.
g. Click **Close** and **OK** to exit out of the properties.
h. Open the **Certificates** folder under the **Console Root**.
i. Right-click on the **Personal** folder and select **All Tasks>>Request New Certificate**.
j. Follow the instructions to generate a certificate request. If there are no certificate templates available you need to edit the certificate template permissions (in **mmc** add the certificate template snap-in,

right-click on the template, select **properties**, and change the permissions for your user) on the certificate authority. The Computer or RAS and IAS templates both work.

k. Once the Certificate is granted by the certificate authority, return to the IAS policy editor to continue the setup.

l. Click **Configure** to configure the certificate for use with the PEAP authentication method. The Protected EAP Properties window appears (figure 11-18).

m. Select the certificate you created in the previous steps, select the EAP types you want to use, and click **OK**.

n. Once the Certificate is granted by the certificate authority, edit the IAS policy.

o. On the **authentication** tab click **authentication methods**.

p. Select **PEAP** and click **Edit**.

q. Select the new certificate and click **Apply**.

r. Click **Configure** to configure the certificate for use with the PEAP authentication method. The Protected EAP Properties window appears, as shown in the following figure:

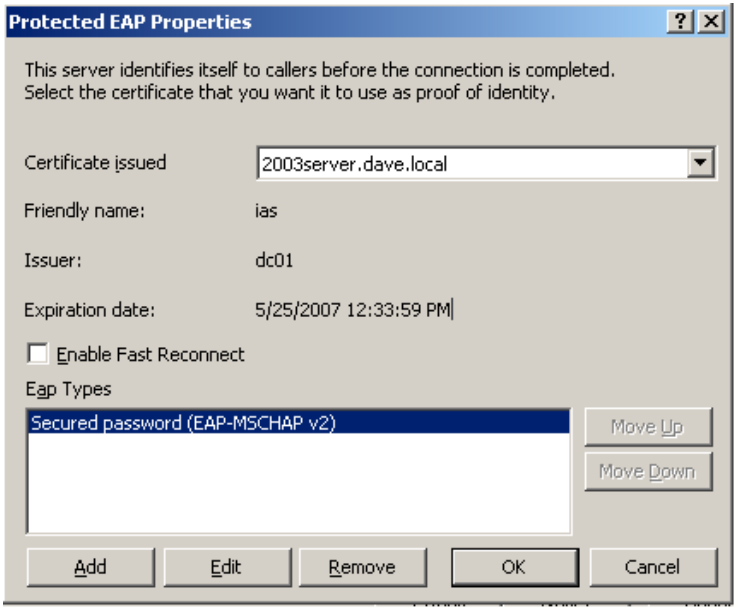


Figure 11-18. Protected EAP Properties

9. Configure the new Remote Access Policy.

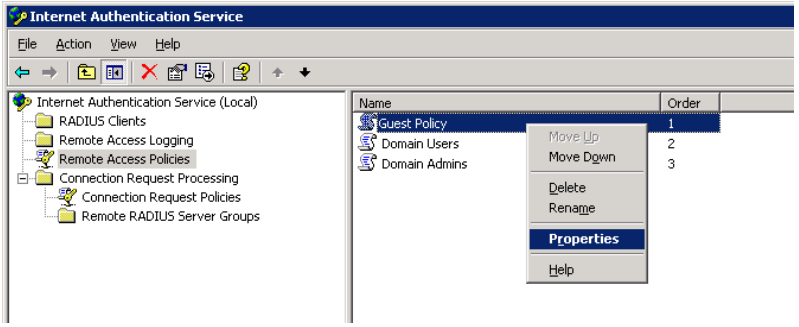


Figure 11-19. IAP, Remote Access Policy, Properties

a. Select **Remote Access Policies**.

b. In the right pane, right-click the new policy name and select **Properties**. The **Guest Policy Properties** window appears:

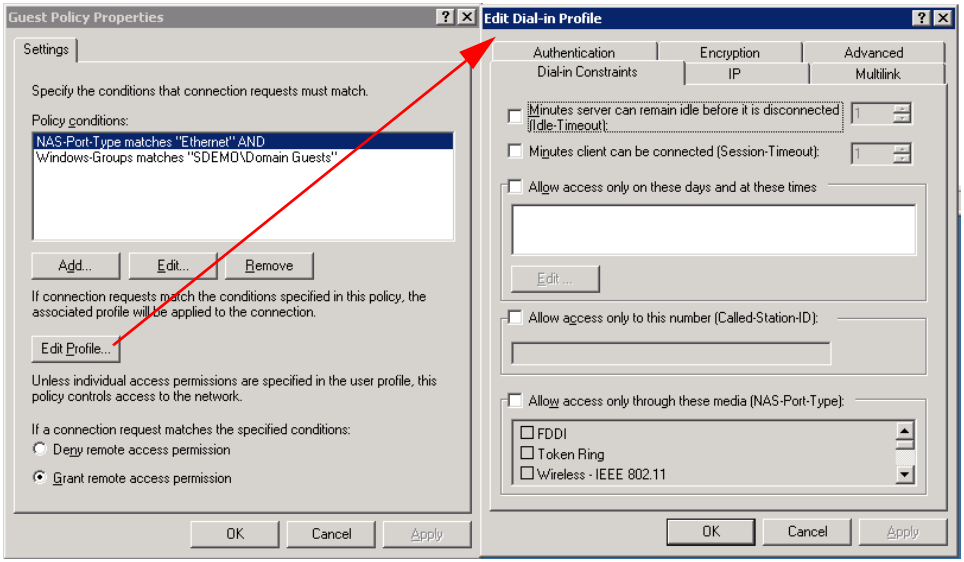


Figure 11-20. IAS, Remote Access Policy, Configure

c. Click **Edit Profile**. The **Edit Dial-in Profile** window appears.
   i. Authentication tab – Select the check boxes for the authentication methods you will allow. This example does not use additional selections.
   ii. Advanced tab – Add three RADIUS attributes:

TIP: The attributes you select might be different for different switch types. Contact ProCurve Networking by HP if you would like assistance.

1) Click **Add**.

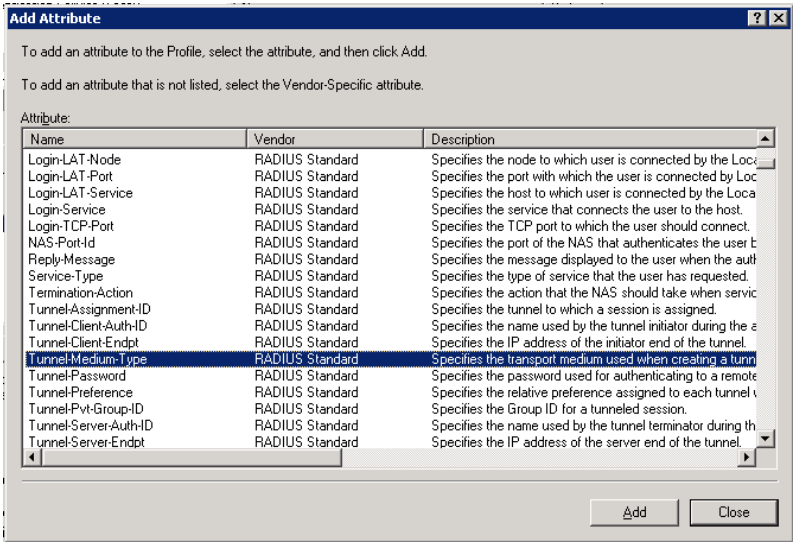

Add Attribute
To add an attribute to the Profile, select the attribute, and then click Add.
To add an attribute that is not listed, select the Vendor-Specific attribute.
Attribute:
Name
Vendor
Description
Login-LAT-Node
Login-LAT-Port
Login-LAT-Service
Login-Service
Login-TCP-Port
NAS-Port-Id
Reply-Message
Service-Type
Termination-Action
Tunnel-Assignment-ID
Tunnel-Client-Auth-ID
Tunnel-Client-Endpt
Tunnel-Medium-Type
Tunnel-Password
Tunnel-Preference
Tunnel-Pvt-Group-ID
Tunnel-Server-Auth-ID
Tunnel-Server-Endpt
RADIUS Standard
Specifies the node to which user is connected by the Loca
Specifies the port with which the user is connected by Loc
Specifies the host to which user is connected by the Loca
Specifies the service that connects the user to the host.
Specifies the TCP port to which the user should connect.
Specifies the port of the NAS that authenticates the user b
Specifies the message displayed to the user when the auth
Specifies the type of service that the user has requested.
Specifies the action that the NAS should take when servic
Specifies the tunnel to which a session is assigned.
Specifies the name used by the tunnel initiator during the a
Specifies the IP address of the initiator end of the tunnel.
Specifies the transport medium used when creating a tunn
Specifies the password used for authenticating to a remote
Specifies the relative preference assigned to each tunnel
Specifies the Group ID for a tunneled session.
Specifies the name used by the tunnel terminator during th
Specifies the IP address of the server end of the tunnel.
Add
Close

Figure 11-21. IAS, Remote Access Policy, Add Attribute

2) Select **Tunnel-Medium-Type**. (Adding the first of the three attributes.)
3) Click **Add**.
4) Click **Add** again on the next window.
5) From the **Attribute value** drop-down list, select **802 (includes all 802 media.**
6) Click **OK**.
7) Click **OK**.
8) Select **Tunnel-Pvt-Group-ID**.
9) Click **Add**.
10) Click **Add** again on the next window. (Adding the second of the three attributes.)

11) In the **Enter the attribute** value area, select the **String** radio button and type the VLAN ID (usually a number such as `50`) in the text box.
12) Click **OK**.
13) Click **OK**.
14) Select **Tunnel-Type**. (Adding the third of the three attributes.)
15) Click **Add**.
16) Click **Add** again on the next window.
17) From the **Attribute value** drop-down list, select **Virtual LANS (VLAN)**.
18) Click **OK**.
19) Click **OK**.
20) Click **OK**.

10. Repeat step 9 for every VLAN group defined in Active Directory.

    IMPORTANT: The order of the connection attributes should be most-specific at the top, and most-general at the bottom.

11. Turn on remote access logging
    a. Click on **Remote Access Logging**.
    b. In the right pane, right-click **Local File**.
    c. Select **Properties**. The Local File Properties window appears:

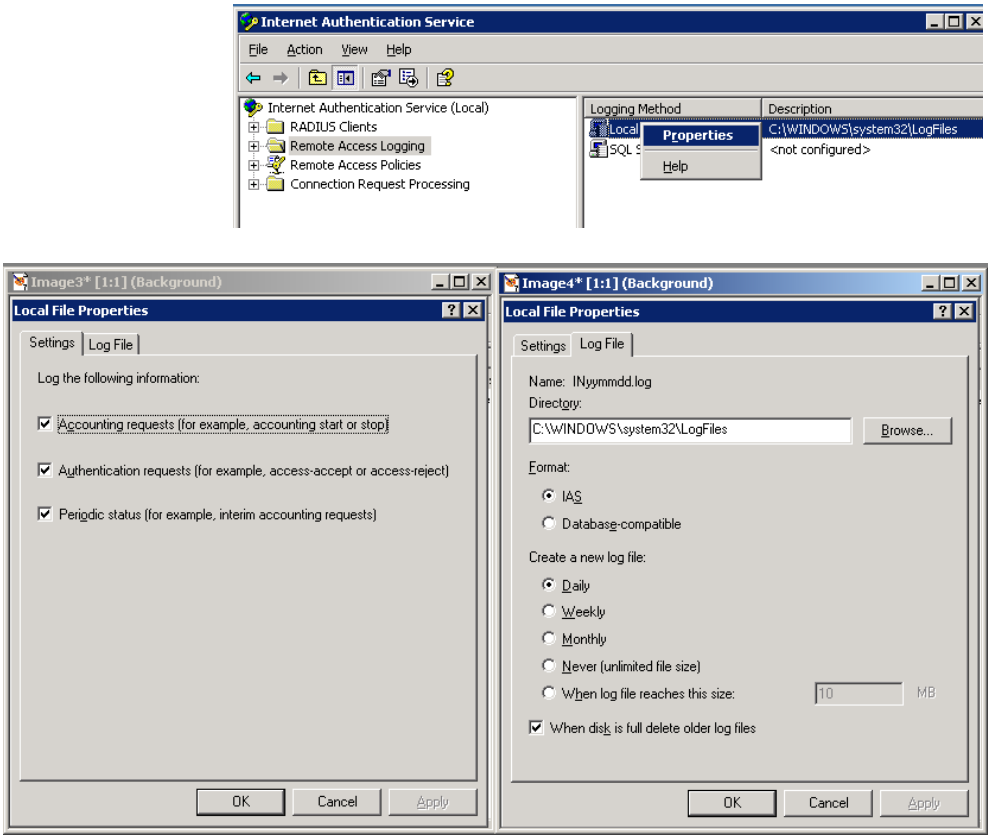


Figure 11-22. IAS, Remote Access Logging Properties

d. Settings tab – Select any of the request and status options you are interested in logging.

e. Log file tab –
   i. In the **Format** area, select the **IAS** radio button.
   ii. In the **Create a new log file** area, select a frequency, such as **Daily**.
   iii. Select the **When disk is full, delete older log files** check box.
   iv. Click **OK**.

12. Install the NAC 800-to-IAS connector – The NAC 800 IAS Connector is a DLL file that is installed on your Windows Server 2003 machine where the IAS component is enabled. The connector is called by IAS after the RADIUS authentication of an endpoint and during the authorization phase. The connector contacts NAC 800 and asks for the posture of the

endpoint. Depending on the posture of the endpoint, the plug-in can return RADIUS attributes to your switch instructing it into which VLAN to place an endpoint. The following figure illustrates this process:

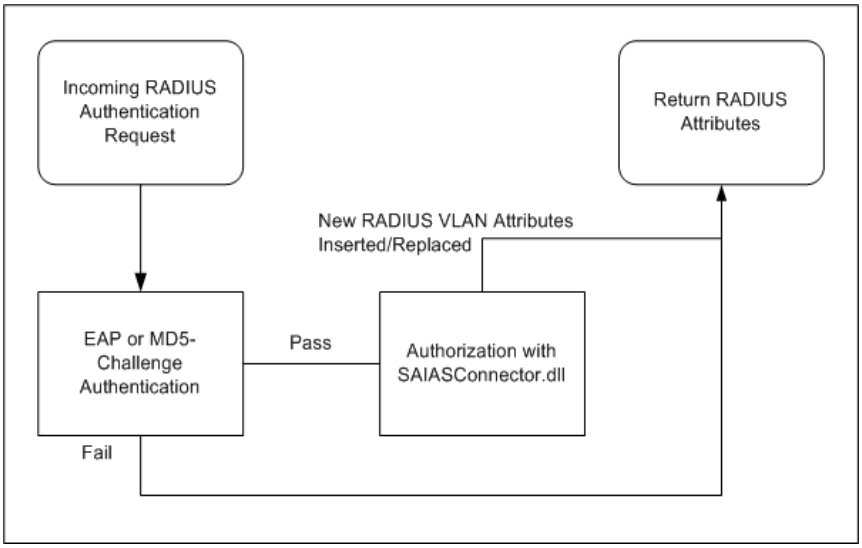


Figure 11-23. NAC 800-to-IAS Connector

a. Copy the following NAC 800 IAS Connector files from the NAC 800 CD-ROM (`/support` directory) to the `WINDOWS/system32` directory on your Windows Server 2003 machine.

   ```
   support/ias/SAIASConnector.dll
   support/ias/SAIASConnector.ini
   ```

b. Import the NAC 800 server's certificate so the connector can communicate with NAC 800 over SSL:
   i. On the Windows Server 2003 machine, click **Start**.
   ii. Select **run**.
   iii. Enter `mmc` .
   iv. Click **OK**.

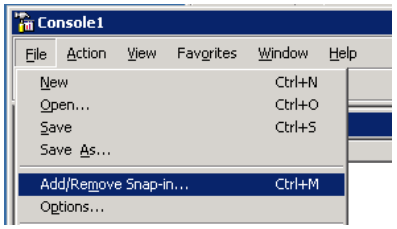


Figure 11-24. IAS, Add/Remove Snap-in

v. Select **File>>Add/Remove Snap-in**.
vi. Click **Add**.

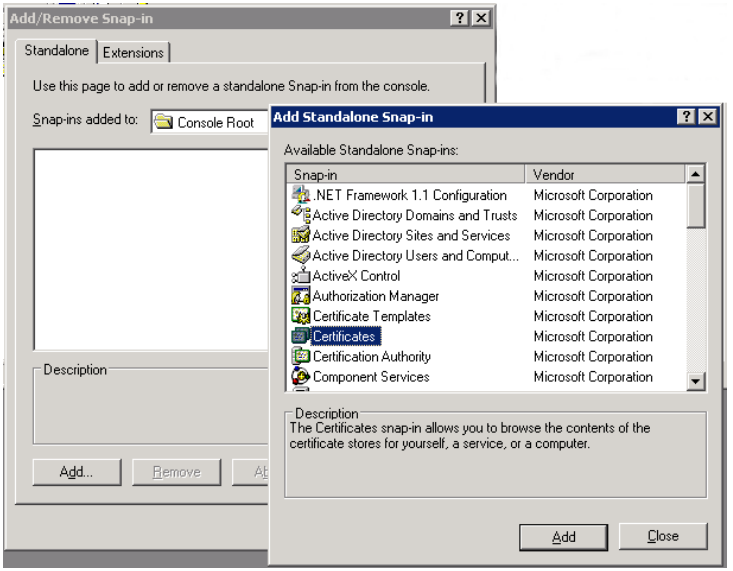

Add/Remove Snap-in
Standalone
Extensions
Use this page to add or remove a standalone Snap-in from the console.
Snap-ins added to: Console Root
Description
Add...
Remove
Add Standalone Snap-in
Available Standalone Snap-ins:
Snap-in
Vendor
.NET Framework 1.1 Configuration Microsoft Corporation
Active Directory Domains and Trusts Microsoft Corporation
Active Directory Sites and Services Microsoft Corporation
Active Directory Users and Comput... Microsoft Corporation
ActiveX Control Microsoft Corporation
Authorization Manager Microsoft Corporation
Certificate Templates Microsoft Corporation
Certificates Microsoft Corporation
Certification Authority Microsoft Corporation
Component Services Microsoft Corporation
Description
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.
Add
Close

Figure 11-25. IAS, Add/Remove Snap-in, Certificates

vii. Select **Certificates**.
viii. Click **Add**.
ix. Select the **Computer account** radio button.
x. Click **Next**.

xi. Select the **Local computer: (the computer this console is running on)** radio button.
xii. Click **Finish**.
xiii. Click **Close**.
xiv. Click **OK**.

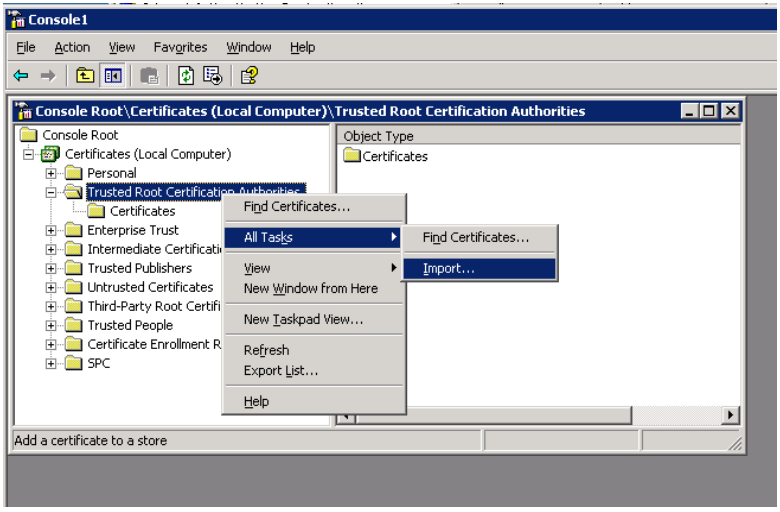


Figure 11-26. IAS, Import Certificate

xv. Right-click on **Console Root>>Certificates (Local Computer)>>Trusted Root Certificate Authorities**.
xvi. Select **All tasks>>import**.
xvii. Click **Next.**
xviii. Click **Browse** and choose the certificate. The NAC 800 server certificate is located on the CD-ROM in

```
support/ias/compliance.keystore.cer
```

xix. Click **Next**.
xx. Click **Next**.
xxi. Click **Finish**.

13. Configure the NAC 800-to-IAS connector –
    a. Modify the INI file for your network environment.

    NAC 800 returns one of postures for an endpoint attempting to

authenticate. For each posture received, a different RADIUS response to the switch can be configured using RADIUS attributes. This response determines into what VLAN the endpoint is placed.

Healthy – The endpoint passed all tests or no failed tests were configured to quarantine.

Checkup – The endpoint failed a test and the action is configured to grant temporary access.

Quarantined – The endpoint failed a test and the action is configured to quarantine.

Unknown – The endpoint has not been tested.

Infected – The endpoint failed the Worms, Virus, and Trojans test.

To configure the response, edit the `SAIASConnector.ini` file. The various settings in the file are listed as follows:

```
--------------------------------------------------------------------------------
      ------
;
; TO DO - Replace <NAS IP> with the IP address of your 802.1X enabled switch
;
[SAIASConnector-<NAS IP>]
;
; TO DO - Replace <SERVER IP> with the IP address of your NAC server
;
[Global]
NASList=192.168.200.135

ServerUrl=https://<SERVER IP>:89/servlet/AccessControlServlet
ServerUrl.1=https://<SERVER IP.1>:89/servlet/AccessControlServlet
ServerUrl.2=https://<SERVER IP.2>:89/servlet/AccessControlServlet
ServerUrl.3=https://<SERVER IP.3>:89/servlet/AccessControlServlet
ServerUrl.4=https://<SERVER IP.4>:89/servlet/AccessControlServlet
ServerUrl.5=https://<SERVER IP.5>:89/servlet/AccessControlServlet
DebugLevel=4
Debug=on
Username=nacuser
Password=nacpwd
;
; If the NAC 800 server cannot be contacted reply to RADIUS with the following
      posture
; 0=healthy, 10=checkup, 20=quarantined, 30=infected, 100=unknown
;

DefaultPosture=0
;
; Use the following timeouts (in milliseconds) for contacting the NAC 800
      server.
```

```
; These timeouts should be coordinated with the RADIUS server and switch
      timeouts for authentication.
;
;ResolveTimeout=0

;ConnectTimeout=60000
;SendTimeout=30000
;ReceiveTimeout=30000

; Use these settings for non-Extreme switches
;
; Uncomment if you want to assign a VLAN for endpoints with a healthy or checkup
      posture

; HealthyRadiusAttributes=Tunnel-Medium-Type,Healthy-Tunnel-Pvt-GroupId,Tunnel-
      Type
; CheckupRadiusAttributes=Tunnel-Medium-Type,Healthy-Tunnel-Pvt-GroupId,Tunnel-
      Type
QuarantineRadiusAttributes=Tunnel-Medium-Type,Quarantine-Tunnel-Pvt-
      GroupId,Tunnel-Type
InfectedRadiusAttributes=Tunnel-Medium-Type,Quarantine-Tunnel-Pvt-
      GroupId,Tunnel-Type
UnknownRadiusAttributes=Tunnel-Medium-Type,Unknown-Tunnel-Pvt-GroupId,Tunnel-
      Type,Unknown-Session-Timeout,Unknown-Termination-Action

;
; Use these settings for Extreme switches
;
; Uncomment if you want NAC 800 to assign a VLAN for endpoints with a healthy or
      checkup posture
; HealthyRadiusAttributes=Healthy
; CheckupRadiusAttributes=Healthy
; QuarantineRadiusAttributes=Quarantine

; InfectedRadiusAttributes=Quarantine
; UnknownRadiusAttributes=Unknown

;
; Policy attributes - In case you want to add attributes to a given policy
      regardless of posture.
; Mainly used because IAS does not contain all standard radius attributes.
; Domain Computers-RadiusAttributes=Unknown-Session-Timeout,Unknown-Termination-
      Action

;
; If you have more than one 802.1X enabled switch, copy the previous section and
      change <NAS IP>
; to that switches IP address. If the other switches have the same settings, use
      the Reference setting.
; For example:
;

; [SAIASConnector-<NAS 2 IP>]
; Reference=SAIASConnector-<NAS 1 IP>
;


;
; The following sections are the RADIUS attributes that will be returned to the
      switch as configured
```

```
; in the <Posture>RadiusAttribute settings above.
;

;

; TO DO - Use these settings for Extreme switches. Change the Value setting to
      match the VLAN names on your switch.
;
[Healthy]
Type=26
VendorId=1916
VendorType=203
DataType=1
Value=Healthy

[Quarantine]
Type=26
VendorId=1916
VendorType=203
DataType=1
Value=Quarantine

[Unknown]
Type=26
VendorId=1916
VendorType=203
DataType=1
Value=Guest

;

; Use the following settings for all non-Extreme switches.
;
[Tunnel-Medium-Type]
Type=65
DataType=3
Value=6

[Tunnel-Type]
Type=64
DataType=3
Value=13

;
; TO DO - Use the following settings for all non-Extreme switches. Change the
      Tunnel-Pvt-GroupId settings
;  to match the VLAN ids on your switch
;

[Healthy-Tunnel-Pvt-GroupId]
Type=81
DataType=1
Value=50

[Healthy-Session-Timeout]
Type=27
DataType=3
Value=3600
```

```
[Healthy-Termination-Action]
Type=29
DataType=3
Value=1

[Quarantine-Tunnel-Pvt-GroupId]
Type=81
DataType=1
Value=15

[Quarantine-Session-Timeout]
Type=27
DataType=3
Value=30

[Quarantine-Termination-Action]
Type=29
DataType=3
Value=1

[Unknown-Tunnel-Pvt-GroupId]
Type=81
DataType=1
Value=5

[Unknown-Session-Timeout]
Type=27
DataType=3
Value=30

[Unknown-Termination-Action]
Type=29
DataType=3
Value=1
-------------------------------------------------------------------------------
      ------
```

b. Enable the Authorization DLL file. At startup, IAS checks the registry for a list of third-party DLL files to call.
   i. Click **Start**.
   ii. Select **Run**.
   iii. Enter `regedit`.
   iv. Navigate to:

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
   ```

   v. Create an `AuthSrv` folder if it does not already exist. (**Edit>>New>>Key**)
   vi. Create a `Parameters` folder inside the `AuthSrv` folder if it does not already exist. (**New>>Key**)
   vii. Right-click on the **Parameters** folder name.
   viii. Select **New>>Multi-string value**.

ix. Type `AuthorizationDLLs` for the name and press **Enter** on the keyboard.
x. Right-click **AuthorizationDLLs**, and select **Modify**.
xi. Enter the following value in the **Value Data** text box.

```
C:\Windows\System32\SAIASConnector.dll
```

xii. Click **OK**.

c. Restart the IAS server (**Start>>Settings>>Control Panel>>Services>>Internet Authentication Services>>Restart**). A log file (`SAIASConnector.log`) is created in the `WINDOWS\system32` directory for debugging purposes.

14. Verify that you are using Microsoft's version of the challenge-handshake authentication protocol (CHAP) MSCHAPv2. If for some reason, you cannot upgrade to MSCHAPv2 at this time, perform the following workaround for MSCHAPv1:

a. Configure passwords:
i. From the Windows Server 2003 machine, select **Start>>Settings>>Control Panel>>Administrative Tools>>Active Directory Users and Computers.**

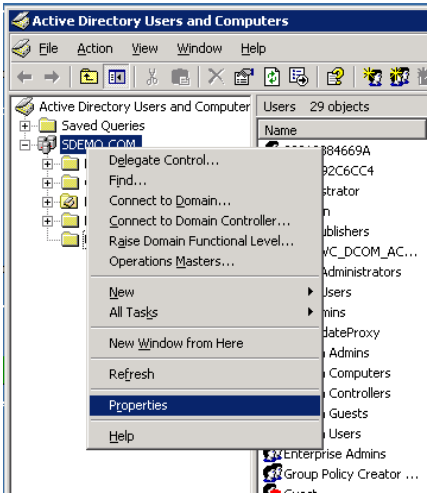


Figure 11-27. Active Directory, properties

ii. Right-click on your directory name and select **Properties**.
iii. Select the **Group Policy** tab.

iv. Click **Open**.
v. Right-click **Default Domain Policy** and select **Edit** (click **OK** if you get a global changes pop-up message).

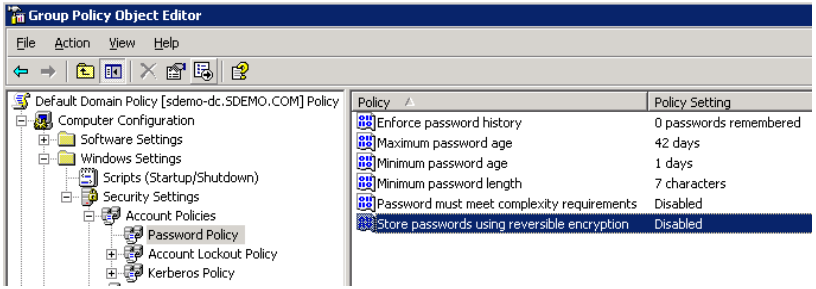


Figure 11-28. Active Directory, Store Passwords

vi. Navigate to **Computer Configuration>>Windows Settings>>Security Settings>>Account Policies>>Password Policy**.
vii. Select **Password Policy**.
viii. Right-click **Store passwords using reversible encryption**.
ix. Select the **Enabled** check box.
x. Click **OK**.
xi. Close the **Group Policy Object Editor** window.
xii. Close the **Group Policy Management** window.
xiii. Close the **<***Active Directory Name***> Properties** window.

15. Create active directory user accounts.
    a. From the Windows Server 2003 machine, select **Start>>Settings>>Control Panel>>Administrative Tools>>Active Directory Users and Computers**.
    b. Right-click on the user's entry under the appropriate domain under **Active Directory Users and Computers.**
    c. Enter the user information requested.
    d. Click **Next**.
    e. Enter the password information.
    f. Click **Next**.
    g. Click **Finish**.
    h. Repeat from step a for all users that need to authenticate using Active Directory.

16. Configure user accounts for Dial-in access and Password Reversible Encryption:
    a. From the Windows Server 2003 machine, select **Start>>Settings>>Control Panel>>Administrative Tools>>Active Directory Users and Computers.**
    b. Click the plus symbol next to the domain to expand the selection.
    c. Select the Users folder.

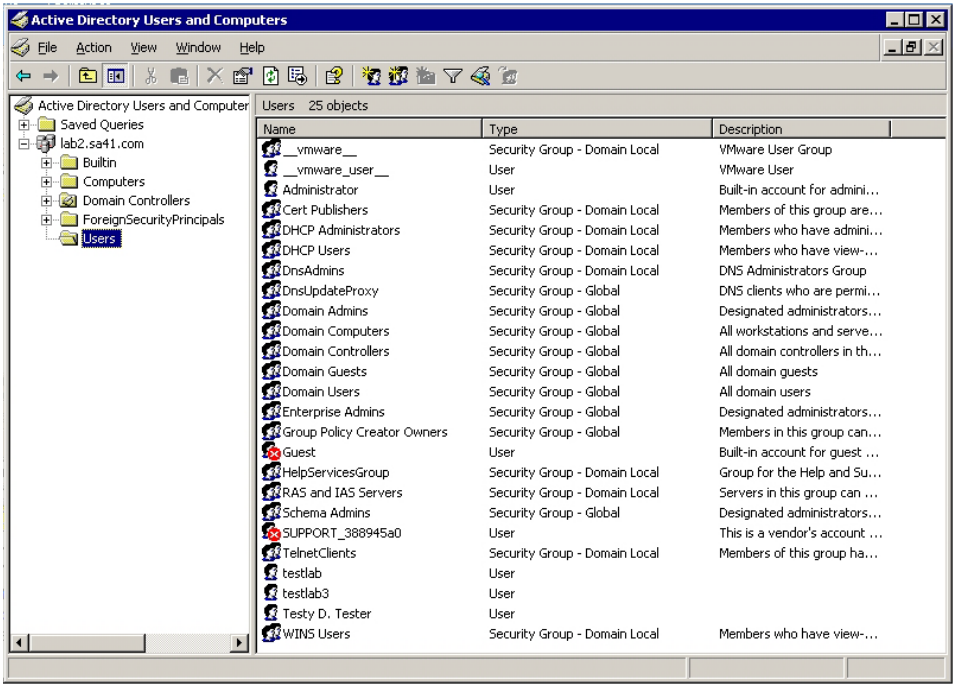

Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computer
Saved Queries
lab2.sa41.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users
Users 25 objects
Name Type Description
__vmware__ Security Group - Domain Local VMware User Group
__vmware_user__ User VMware User
Administrator User Built-in account for admini...
Cert Publishers Security Group - Domain Local Members of this group are...
DHCP Administrators Security Group - Domain Local Members who have admini...
DHCP Users Security Group - Domain Local Members who have view-...
DnsAdmins Security Group - Domain Local DNS Administrators Group
DnsUpdateProxy Security Group - Global DNS clients who are permi...
Domain Admins Security Group - Global Designated administrators...
Domain Computers Security Group - Global All workstations and serve...
Domain Controllers Security Group - Global All domain controllers in th...
Domain Guests Security Group - Global All domain guests
Domain Users Security Group - Global All domain users
Enterprise Admins Security Group - Global Designated administrators...
Group Policy Creator Owners Security Group - Global Members in this group can...
Guest User Built-in account for guest ...
HelpServicesGroup Security Group - Domain Local Group for the Help and Su...
RAS and IAS Servers Security Group - Domain Local Servers in this group can ...
Schema Admins Security Group - Global Designated administrators...
SUPPORT_388945a0 User This is a vendor's account ...
TelnetClients Security Group - Domain Local Members of this group ha...
testlab User
testlab3 User
Testy D. Tester User
WINS Users Security Group - Domain Local Members who have view-...

Figure 11-29. Active Directory Users and Computers Window

    d. Right-click a user name and select **Properties**. The Properties windows appears:

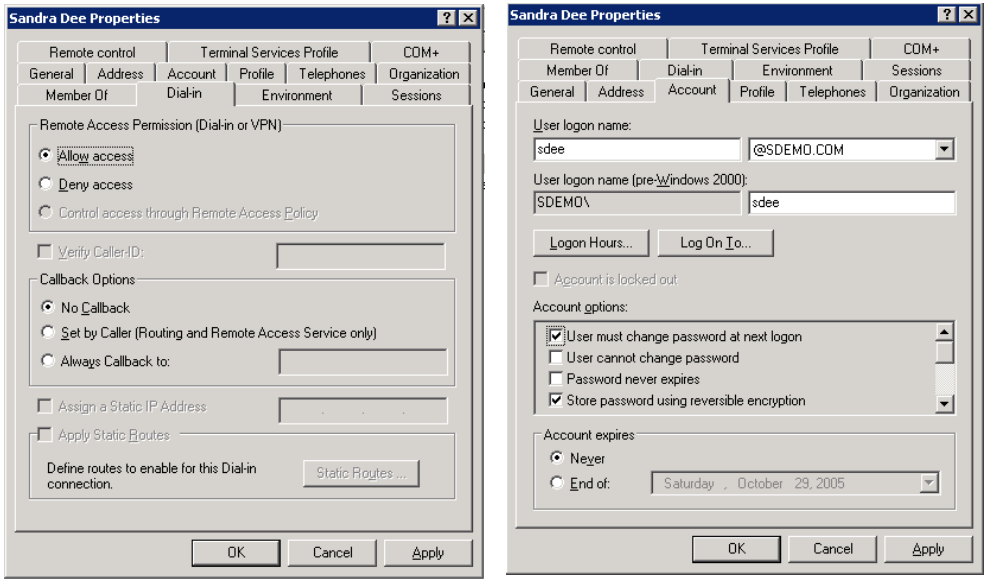


Figure 11-30. Active Directory, User Account Properties

e. Select the **Dial-in** tab.

f. In the **Remote Access Permission** area, select the **Allow Access** radio button.

g. Select the **Account** tab.

h. Verify that you are using Microsoft's version of the challenge-handshake authentication protocol (CHAP) MSCHAPv2. If for some reason, you cannot upgrade to MSCHAPv2 at this time, perform the following workaround for MSCHAPv1:

   In the **Account options** area, select the **Store password using reversible encryption** check box.

NOTE: If there are existing user accounts in your Active Directory installation when you enable reversible encryption, the passwords must be reset (either by the user or by the system administrator) before reversible encryption takes effect.

i. Click **OK**.

j. Repeat from step a for each user account.

Proxying RADIUS Requests to an Existing RADIUS Server Using the Built-in NAC 800 RADIUS Server

TIP: For an explanation of how the components communicate, see "NAC 800 and 802.1X" on page 11-4.

To configure NAC 800 to proxy RADIUS requests to an existing RADIUS server:

1. To configure the RADIUS server to proxy requests to your existing RADIUS server:
   a. Log in to the ES as `root` via SSH.
   b. Open the following file with a text editor such as `vi`:

      ```
      /etc/raddb/proxy.conf
      ```

   c. Append the following section replacing the parameters in <> with your RADIUS servers information:

      ```
      realm NULL {
      type= radius
      authhost= <RADIUS host or IP>:<RADIUS auth port>
      accthost= <RADIUS host or IP>:<RADIUS acct port>
      secret= <the shared secret for your RADIUS server>
      }
      ```

   d. Save and exit the file.

NOTE: The realm NULL section must go after the realm LOCAL section, or you can comment out the realm LOCAL section.

2. Configure your RADIUS server to allow the NAC 800 IP address as a client with the shared secret specified in the previous step. See your RADIUS server's documentation for instructions on how to configure allowed clients.

3. Configure the `SAFreeRADIUSConnector.conf` file with the appropriate RADIUS attributes and VLANS. See comments in the following sample file for instructions.

```
#
# Free Radius Connector configuration file
#

#
# TO DO - Change localhost to your server's IP if this is not the built-in
      FreeRadius server
#


ServerUrl=https://localhost/servlet/AccessControlServlet
DebugLevel=4
Debug=on
Username=nacuser
Password=nacpwd

#
# TO DO - Modify the vlan ids and names to match your switch configuration
#



#
# Use these attributes for all non-Extreme switches
#

#
# Uncomment these two sections if you want the connector to specify the normal user
      vlan
# rather than specifying it for each user in the users configuration file.
#


#"HealthyRadiusAttributes"
#       Tunnel-Medium-Type := 6,
#       Tunnel-Private-Group-ID := 50,
#       Tunnel-Type := VLAN,
#
#"CheckupRadiusAttributes"
#       Tunnel-Medium-Type := 6,
#       Tunnel-Private-Group-ID := 50,
#       Tunnel-Type := VLAN,
```

```
"QuarantineRadiusAttributes"
      Tunnel-Medium-Type := 6,
      Tunnel-Private-Group-ID := 15,
      Tunnel-Type := VLAN,

"InfectedRadiusAttributes"
      Tunnel-Medium-Type := 6,
      Tunnel-Private-Group-ID := 15,
      Tunnel-Type := VLAN,



"UnknownRadiusAttributes"
      Tunnel-Medium-Type := 6,
      Tunnel-Private-Group-ID := 5,
      Tunnel-Type := VLAN,


#
# Use these attributes for Extreme switches
#


#"HealthyRadiusAttributes"
#      Extreme-Netlogin-Vlan := HealthyVlanName
#
#"CheckupRadiusAttributes"
#      Extreme-Netlogin-Vlan := HealthyVlanName
#
#"QuarantineRadiusAttributes"
#      Extreme-Netlogin-Vlan := QuarantineVlanName
#


#"InfectedRadiusAttributes"
#      Extreme-Netlogin-Vlan := QuarantineVlanName
#
#"UnknownRadiusAttributes"
#      Extreme-Netlogin-Vlan := TempOrGuestVlanName




#
# TO DO - Uncomment if you want different switches to have different attributes.
#      Posture is Healthy, Checkup, Quarantine, Infected, or Unknown.
#      This entry must come after the default set of attributes in the file.
#
#"<POSTURE>RadiusAttributes-<NAS IP ADDRESS>"
#      Tunnel-Medium-Type := 6,
#      Tunnel-Private-Group-ID := 15,
#      Tunnel-Type := VLAN,
```

4. Test the RADIUS server proxy:

   ```
   radtest <user> <passwd> <radius-server[:port]> <nas-port-number><secret>
   ```

Using the Built-in NAC 800 RADIUS Server for Authentication

If you selected the **Manual End-user authentication method** in the **Authentication settings** area of the **System configuration>>Quarantining>>802.1X** window, configure NAC 800 according to the instructions in this section.

To configure NAC 800 to handle RADIUS requests:

Add users to the RADIUS server by modifying the `/etc/raddb/users` file. Add user entries to the beginning of the file in the following format:

Clear text authentication:

```
<user name> Auth-Type := Local, User-Password =="password"
```

EAP, PEAP, or MD5-Challenge authentication (the built-in windows 802.1X supplicant uses these methods):

```
<user name> Auth-Type := EAP, User-Password =="password"
```

For example:

```
dave Auth-Type := EAP, User-Password =="d@9ij8!e"
```

Configuring Non-HP Switches

If you have an HP appliance and non-HP switches, you will need to add these sections to the .conf (for FreeRADIUS) or .ini files (for IAS).

To configure for non-HP switches:

Configure the `SAFreeRadiusConnector.conf` file with the appropriate radius attributes and VLANS. See comments in the sample file below for instructions:

NOTE: When using the Cisco® Catalyst® 6509 with the Catalyst operating system (CatOS), you need to refer to the VLAN by name, and not by number as shown in the following sample file. For example, use "Tunnel-Private-Group-ID := User_Seg_PA," instead of "Tunnel-Private-Group-ID := 50,".

```
#
# NAC 800 Free Radius Connector configuration file
#

#
# General configuration parameters
#
ServerUrl=https://<SERVER IP>:89/servlet/AccessControlServlet
ServerUrl.1=https://<SERVER IP.1>:89/servlet/AccessControlServlet
ServerUrl.2=https://<SERVER IP.2>:89/servlet/AccessControlServlet
ServerUrl.3=https://<SERVER IP.3>:89/servlet/AccessControlServlet
ServerUrl.4=https://<SERVER IP.4>:89/servlet/AccessControlServlet
ServerUrl.5=https://<SERVER IP.5>:89/servlet/AccessControlServlet

DebugLevel=4
Debug=on
Username=nac
Password=changeme

#
# TO DO - Modify the vlan ids and names to match your switch configuration
#

#
# Use these attributes for all non-Extreme switches
#

#

# Uncomment these two sections if you want the connector to specify the
normal user vlan
# rather than specifying it for each user in the users configuration file.
#
#"HealthyRadiusAttributes"
#        Tunnel-Medium-Type := 6,
#        Tunnel-Private-Group-ID := 50,
#        Tunnel-Type := VLAN,
```

```
#
#"CheckupRadiusAttributes"
#        Tunnel-Medium-Type := 6,
#        Tunnel-Private-Group-ID := 50,
#        Tunnel-Type := VLAN,

"QuarantineRadiusAttributes"
        Tunnel-Medium-Type := 6,
        Tunnel-Private-Group-ID := 15,
        Tunnel-Type := VLAN,


"InfectedRadiusAttributes"
        Tunnel-Medium-Type := 6,
        Tunnel-Private-Group-ID := 15,
        Tunnel-Type := VLAN,

"UnknownRadiusAttributes"
        Tunnel-Medium-Type := 6,
        Tunnel-Private-Group-ID := 5,
        Tunnel-Type := VLAN,



#
# Use these attributes for Extreme switches
#
#"HealthyRadiusAttributes"
#        Extreme-Netlogin-Vlan := HealthyVlanName
#
#"CheckupRadiusAttributes"
#        Extreme-Netlogin-Vlan := HealthyVlanName
#

#"QuarantineRadiusAttributes"
#        Extreme-Netlogin-Vlan := QuarantineVlanName
#
#"InfectedRadiusAttributes"
#        Extreme-Netlogin-Vlan := QuarantineVlanName
#
#"UnknownRadiusAttributes"
#        Extreme-Netlogin-Vlan := TempOrGuestVlanName




#
# TO DO - Uncomment if you want different switches to have different
attributes.
#        Posture is Healthy, Checkup, Quarantine, Infected, or Unknown.
#        This entry must come after the default set of attributes in the
file.
```

```
#
#"<POSTURE>RadiusAttributes-<NAS IP ADDRESS>"
#         Tunnel-Medium-Type := 6,
#         Tunnel-Private-Group-ID := 15,
#         Tunnel-Type := VLAN,
```

Enabling NAC 800 for 802.1X

To enable NAC 800 for use in an 802.1X network, you need to select it in the console, and make a few changes to the properties using JMS and an XML file.

NAC 800 Console Configuration

To enable 802.1X in the NAC 800 console:

NAC 800 Home window>>System configuration>>Quarantining

1. In the **Select a quarantine method** area, select the **802.1X** quarantine method radio button.

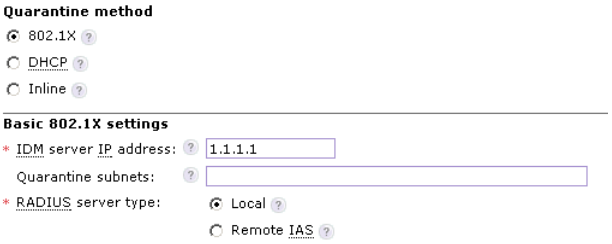


Figure 11-31. Enabling 802.1X in the Console

2. In 802.1X enforcement mode, the Enforcement servers must be able watch DHCP conversations and detect endpoints by sniffing network traffic as it flows between the DHCP server and the endpoints. Select one of the following radio buttons:
   - **remote** – Disables the local RADIUS server so that an IAS server configured with the NAC IAS plug-in to point to an enforcement server can be used instead. When possible, a local RADIUS server that proxies to the IAS server should be the preferred configuration.

- **local** – In simple configurations, it is possible to span, or mirror, the switch port into which the DHCP server is connected. The eth1 interface of the Enforcement server is then plugged into the spanned port and endpoint traffic is monitored on the eth1 interface. In this case, choose the local option.

3. Click **OK**.

Setting Up the Supplicant

Now you must enable the endpoint for 802.1X. If you do not, the endpoint can never pass the initial challenge from the switch, as the switch searches for an 802.1X-enabled endpoint. This sections describes how to set up the following endpoints for 802.1X:

- Windows XP Professional endpoint
- Windows XP Home endpoint
- Windows 2000 Professional endpoint

How to enable a Windows XP Professional endpoint for 802.1X:

Windows main window>>Start>>Settings>>Network Connections

1. Right-click on **Local Area Connection**. The **Local Area Connection** windows appears:
2. Select **Properties**.

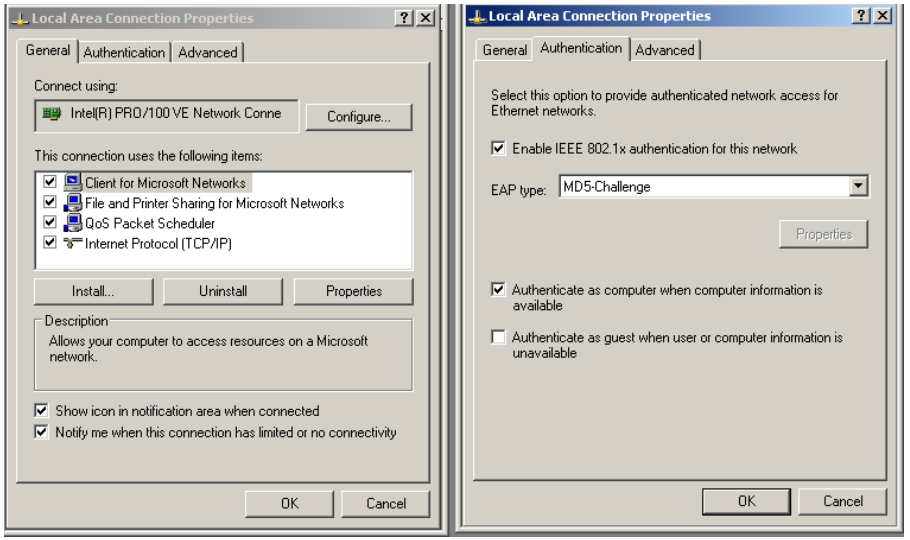


Figure 11-32. IAS, Windows Client Authentication

3. General tab –
   a. Select the **Show icon in notification area when connected** check box. This enables the **Windows XP balloon help** utility, which can assist you when entering information and troubleshooting errors.
4. Authentication tab –
   a. Select the **Enable IEE 802.1X authentication for this network** check box.
   b. Select an EAP type from the drop-down list. For this example, select **MD5-Challenge**.

      Important: This EAP type must match the EAP type selected in step 7, step q on page 11-19.
   c. Clear or select the **Authenticate as computer when computer information is** available check box. The choice is yours.
5. Click **OK**.
6. Select to reboot if necessary.

How to enable a Windows XP Home endpoint for 802.1X:

Windows Main Window>>Start>>Settings>>Control Panel>>Administrative Tools>>Services

1. Wireless Zero Configuration (this service needs to be started, if not already running the user needs to right-click on the service named Wireless Zero Configuration and click 'start').
2. Right-click on **Local Area Connection**. The **Local Area Connection** windows appears, as shown in Figure 11-32 on page 11-45.
3. Select **Properties** (Figure 11-32 on page 11-45).
4. General tab –
   a. Select the **Show icon in notification area when connected** check box. This enables the **Windows XP balloon help** utility, which can assist you when entering information and troubleshooting errors.
5. Authentication tab –
   a. Select the **Enable IEE 802.1X authentication for this network** check box.
   b. Select an EAP type from the drop-down list. For this example, select **MD5-Challenge**.

      Important: This EAP type must match the EAP type selected in “Setting up the RADIUS Server”, step 7, step q on page 11-19.
   c. Clear or select the **Authenticate as computer when computer information is** available check box. The choice is yours.
6. Click **OK**.
7. Select to reboot if necessary.

How to enable a Windows 2000 Professional endpoint for 802.1X:

Windows Main Window-> Start-> Settings->Control Panel>>Administrative Tools>>Services

1. Wireless Configuration (this service needs to be started, if not already running the user needs to right-click on the service named Wireless Configuration and click 'start').
2. Right-click on **Local Area Connection**. The **Local Area Connection** windows appears, as shown in Figure 11-32 on page 11-45.
3. Select **Properties** (Figure 11-32 on page 11-45).
4. General tab –

a. Select the **Show icon in notification area when connected** check box. This enables the **Windows XP balloon help** utility, which can assist you when entering information and troubleshooting errors.

5. Authentication tab –
   a. Select the **Enable IEE 802.1X authentication for this network** check box.
   b. Select an EAP type from the drop-down list. For this example, select **MD5-Challenge**.

      IMPORTANT: This EAP type must match the EAP type selected in "Setting up the RADIUS Server", step 7, step q on page 11-19.
   c. Clear or select the **Authenticate as computer when computer information is** available check box. The choice is yours.
6. Click **OK**.
7. Select to reboot if necessary.

Setting Up the Authenticator

This section provides sample configurations for the following switches:

- "Cisco® 2950 IOS" on page 11-47
- "Cisco® 4006 CatOS" on page 11-48
- "Enterasys® Matrix 1H582-25" on page 11-49
- "Extreme® Summit 48si" on page 11-49
- "ExtremeWare" on page 11-50
- "ExtremeXOS" on page 11-50
- "Foundry® FastIron® Edge 2402" on page 11-51
- "HP ProCurve® 420AP" on page 11-51
- "HP ProCurve® 530AP" on page 11-52
- "HP ProCurve® 3400/3500/5400" on page 11-53
- "Nortel® 5510" on page 11-54

The lines that apply to 802.1X are shown in *`green italic text`*. Make sure that you add this information when configuring your switch.

Cisco® 2950 IOS

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
```

```
dot1x system-auth-control
interface FastEthernet0/1
  switchport mode access
  dot1x port-control auto
  dot1x timeout quiet-period 30
  dot1x guest-vlan 5
  dot1x reauthentication
  spanning-tree portfast
!
interface FastEthernet0/2
  switchport mode access
  dot1x port-control auto
  dot1x timeout quiet-period 30
  dot1x guest-vlan 5
  dot1x reauthentication
  spanning-tree portfast
!
interface FastEthernet0/3
  switchport mode access
  dot1x port-control auto
  dot1x timeout quiet-period 30
  dot1x guest-vlan 5
  dot1x reauthentication
  spanning-tree portfast
!
interface FastEthernet0/4
  switchport mode access
  dot1x port-control auto
  dot1x timeout quiet-period 30
  dot1x guest-vlan 5
  dot1x reauthentication
  spanning-tree portfast

ip http server
radius-server host 10.11.100.10 auth-port 1812 acct-port 1813
      key mysecretpassword
radius-server retransmit 3
!
```

Cisco® 4006 CatOS

```
set dot1x re-authperiod 100
set feature dot1x-radius-keepalive disable

#radius
set radius server 172.17.20.150 auth-port 1812 primary
set radius key mysecretpassword
!

#module 2 : 48-port 10/100BaseTx Ethernet
set port dot1x 2/15 port-control auto
set port dot1x 2/17 port-control auto
set port dot1x 2/18 port-control auto
set port dot1x 2/19 port-control auto
set port dot1x 2/15 re-authentication enable
set port dot1x 2/17 re-authentication enable
set port dot1x 2/18 re-authentication enable
set port dot1x 2/19 re-authentication enable
```

```
set port dot1x 2/15 guest-vlan 40
set port dot1x 2/17 guest-vlan 40
set port dot1x 2/18 guest-vlan 40
set port dot1x 2/19 guest-vlan 40
```

Enterasys® Matrix 1H582-25

```
! dot1x
  set dot1x auth-config authcontrolled-portcontrol forced-
      auth fe.0.5-24
  set dot1x auth-config maxreq 10000 fe.0.1-4
  set dot1x auth-config keytxenabled true fe.0.1-4
  set dot1x enable
!

! radius
  set radius timeout 30
set radius server 1 10.11.100.10 1812
       02108000AE5BA9C47EDC24F2CA6529EE4CCC8930B
BD70F5AAA2CF0C5DBAA5DA97FADFE95
  set radius enable
!
```

Extreme® Summit 48si

TIP: When authenticating via the onboard FreeRadius server, you need to add the administrative line in the RADIUS users file.

TIP: Change the admin password to a non-blank password.

```
create vlan "Operations"
create vlan "CommandControl"
create vlan "Quarantine"
create vlan "Guest"
create vlan "Temp"

# Radius configuration
#
enable radius
configure radius primary shared-secret encrypted
       "ouzoisgprdr#s{fqa"
configure radius primary server 10.10.100.10 1645 client-ip
       10.10.100.1


# Network Login Configuration
configure vlan Temp dhcp-address-range 10.10.5.100 -
       10.10.5.150
configure vlan Temp dhcp-options default-gateway 10.10.5.1
configure vlan Temp dhcp-options dns-server 10.10.100.11
configure vlan Temp dhcp-options wins-server 10.10.100.10
enable netlogin port 33 vlan Temp
enable netlogin port 34 vlan Temp
enable netlogin port 35 vlan Temp
```

```
enable netlogin port 36 vlan Temp
enable netlogin port 37 vlan Temp
enable netlogin port 38 vlan Temp
enable netlogin port 39 vlan Temp
enable netlogin port 40 vlan Temp
configure netlogin redirect-page "https://10.10.100.100:89"
```

ExtremeWare

TIP: When authenticating via the onboard FreeRadius server, you need to add the administrative line in the RADIUS users file.

TIP: Change the admin password to a non-blank password.

```
create vlan "Quarantine"
create vlan "Test"
# Radius configuration
#
enable radius
configure radius primary shared-secret encrypted
      "ouzoisgprdr#s{fqa"
configure radius primary server 10.50.32.10 1812 client-ip
      10.50.32.254

# Network Login Configuration
enable netlogin port 1 vlan Default
enable netlogin port 2 vlan Default
enable netlogin port 3 vlan Default
enable netlogin port 4 vlan Default
enable netlogin port 5 vlan Default
enable netlogin port 6 vlan Default
enable netlogin port 7 vlan Default
enable netlogin port 8 vlan Default
configure netlogin mac auth-retry-count 3
configure netlogin mac reauth-period 1800
```

ExtremeXOS

```
#
create vlan "Quarantine"
create vlan "Test"

enable radius netlogin
configure radius netlogin timeout 3

configure radius-accounting netlogin timeout 3

# Module netLogin configuration.
#
configure netlogin vlan Test
enable netlogin dot1x mac
enable netlogin ports 1-8 dot1x
configure netlogin dot1x timers server-timeout 30 quiet-
      period 60 reauth-period
```

```
100 supp-resp-timeout 30
configure netlogin dot1x eapol-transmit-version v1
configure netlogin dot1x guest-vlan Guest
enable netlogin logout-privilege
enable netlogin session-refresh 3
configure netlogin base-url "network-access.com"
configure netlogin redirect-page "http://
      www.extremenetworks.com"
configure netlogin banner ""
```

Foundry® FastIron® Edge 2402

```
dot1x-enable
  auth-fail-action restricted-vlan
  auth-fail-vlanid 5
  mac-session-aging no-aging permitted-mac-only
  enable ethe 1 to 4

aaa authentication dot1x default radius

radius-server host 10.11.100.10 auth-port 1812 acct-port 1813
      default key 1 $6\-ndUnoS!--+sU@

interface ethernet 1
  dot1x port-control auto
  sflow-forwarding
!
interface ethernet 2
  dot1x port-control auto
  sflow-forwarding
!
interface ethernet 3
  dot1x port-control auto
  sflow-forwarding
!
interface ethernet 4
  dot1x port-control auto
  sflow-forwarding
!
```

HP ProCurve® 420AP

This section shows how to configure the security settings on the 420AP so that user access may be controlled using Dynamic VLAN provisioning.

```
HP ProCurve Access Point 420#configure
HP ProCurve Access Point 420(config)#interface ethernet
Enter Ethernet configuration commands, one per line.
HP ProCurve Access Point 420(if-ethernet)#no ip dhcp
HP ProCurve Access Point 420(if-ethernet)#ip address <IP of
      Access Point Netmask Gateway>
HP ProCurve Access Point 420(if-ethernet)#end
HP ProCurve Access Point 420(config)#management-vlan 200
      tagged
HP ProCurve Access Point 420(config)#interface wireless g
```

```
Enter Wireless configuration commands, one per line.
HP ProCurve Access Point 420(if-wireless-g)#ssid index 1
HP ProCurve Access Point 420(if-wireless-g-ssid-1)#closed-
      system
HP ProCurve Access Point 420(if-wireless-g-ssid-1)#radius-
      authentication-server address <IP of RADIUS Server>
HP ProCurve Access Point 420(if-wireless-g-ssid-1)#radius-
      authentication-server key <Shared RADIUS secret>
HP ProCurve Access Point 420(if-wireless-g-ssid-1)#radius-
      authentication-server vlan-format ascii
HP ProCurve Access Point 420(if-wireless-g-ssid-1)#ssid
      Enterprise420
HP ProCurve Access Point 420(if-wireless-g-ssid-1)#vlan 100
      tagged
HP ProCurve Access Point 420(if-wireless-g-ssid-1)#security-
      suite 6 wpa-wpa2
HP ProCurve Access Point 420(if-wireless-g-ssid-1)#enable
HP ProCurve Access Point 420(if-wireless-g-ssid-1)#end
HP ProCurve Access Point 420(if-wireless-g)#end
HP ProCurve Access Point 420(config)#radius-accounting
      address <IP of RADIUS Server>
HP ProCurve Access Point 420(config)#radius-accounting key
      <Shared RADIUS secret>
HP ProCurve Access Point 420(config)#radius-accounting enable
HP ProCurve Access Point 420(config)#vlan enable dynamic
Reboot system now? <y/n>: y
```

Dynamic WEP: Enter the same commands as the previous configuration; however, substitute `security-suite 5` instead of `security-suite 6 wpa-wpa2`.

HP ProCurve® 530AP

This section shows how to configure the security settings on the 530AP so that user access `may be controlled using Dynamic VLAN provisioning.`

```
ProCurve Access Point 530#conf
ProCurve Access Point 530(config)#interface ethernet
ProCurve Access Point 530(ethernet)#ip address <IP of Access
      Point > Netmask
ProCurve Access Point 530(ethernet)#ip default-gateway <IP of
      Gateway>
ProCurve Access Point 530(ethernet)#management-vlan 200
ProCurve Access Point 530(ethernet)#untagged-vlan 200
ProCurve Access Point 530(radio1-wlan1)#ssid Enterprise530
ProCurve Access Point 530(radio1-wlan1)#closed
ProCurve Access Point 530(radio1-wlan1)#vlan 100
ProCurve Access Point 530(radio1-wlan1)#security wpa-8021x
ProCurve Access Point 530(radio1-wlan1)#radius primary ip <IP
      of RADIUS Server>
The RADIUS shared secret key must also be set to enable
      communication between this
device and the RADIUS server.
ProCurve Access Point 530(radio1-wlan1)#radius primary key
      <Shared RADIUS secret>
```

```
ProCurve Access Point 530(radio1-wlan1)#radius-accounting
      primary ip <IP of RADIUS Server>
ProCurve Access Point 530(radio1-wlan1)#radius-accounting
      primary key<Shared RADIUS secret>
ProCurve Access Point 530(radio1-wlan1)#wpa-cipher-aes
ProCurve Access Point 530(radio1-wlan1)#write mem
ProCurve Access Point 530(radio1-wlan1)#enable
ProCurve Access Point 530(radio1-wlan1)#enable
ProCurve Access Point 530(config)#radio 1
ProCurve Access Point 530(radio1)#enable
ProCurve Access Point 530(radio1)#radio 2
ProCurve Access Point 530(radio2)#enable
ProCurve Access Point 530(config)#write mem
ProCurve Access Point 530(config)#exit
```

Dynamic WEP: `ProCurve Access Point 530#conf`

```
ProCurve Access Point 530(config)#interface ethernet
ProCurve Access Point 530(ethernet)#ip address <IP of Access
      Point > Netmask
ProCurve Access Point 530(ethernet)#ip default-gateway <IP of
      Gateway>
ProCurve Access Point 530(ethernet)#management-vlan 200
ProCurve Access Point 530(ethernet)#untagged-vlan 200
ProCurve Access Point 530(radio1-wlan1)#ssid Enterprise530
ProCurve Access Point 530(radio1-wlan1)#closed
ProCurve Access Point 530(radio1-wlan1)#vlan 100
ProCurve Access Point 530(radio1-wlan1)#security dynamic-wep
ProCurve Access Point 530(radio1-wlan1)#radius primary ip <IP
      of RADIUS Server>
The RADIUS shared secret key must also be set to enable
      communication between this device and the RADIUS
      server.
ProCurve Access Point 530(radio1-wlan1)#radius primary key
      <Shared RADIUS secret>
ProCurve Access Point 530(radio1-wlan1)#radius-accounting
      primary ip <IP of RADIUS Server>
The RADIUS shared secret key must also be set to enable
      communication between this device and the RADIUS
      server.
ProCurve Access Point 530(radio1-wlan1)#radius-accounting
      primary key<Shared RADIUS secret>
ProCurve Access Point 530(radio1-wlan1)#wep-key-ascii
      ProCurve Access Point 530(radio1-wlan1)#wep-key-1
      1q2w3e4r5t6y7
ProCurve Access Point 530(radio1-wlan1)#write mem
ProCurve Access Point 530(radio1-wlan1)#enable
ProCurve Access Point 530(radio2-wlan1)#enable
ProCurve Access Point 530(config)#radio 1
ProCurve Access Point 530(radio1)#enable
ProCurve Access Point 530(radio1)#radio 2
ProCurve Access Point 530(radio2)#enable
ProCurve Access Point 530(config)#write mem
ProCurve Access Point 530(config)#exit
```

HP ProCurve® 3400/3500/5400

```
radius-server host 10.60.1.3 key hpsecret
```

```
aaa accounting network start-stop radius
aaa authentication port-access eap-radius
aaa port-access authenticator 1-8
aaa port-access authenticator 1-8 auth-vid 100
aaa port-access authenticator 1-8 unauth-vid 101
aaa port-access authenticator active
```

Nortel® 5510

NOTE: When the Nortel switch is used in unstacked mode, a range of ports is defined as 1-24.
When the Nortel switch is used in stacked mode, a range of ports is defined as 1/1-24; <unit>/<port-port>. See the Nortel switch user manuals for more information.

```
Radius Server setup:

radius-server host 10.0.0.5
radius-server secondary-host 0.0.0.0
radius-server port 1812
! radius-server key ********


Enable 802.1X:

eapol enable
interface FastEthernet ALL
eapol port 1-2 status auto traffic-control in-out re-
      authentication enable re-a
uthentication-period 3600 re-authenticate quiet-interval 60
      transmit-interval 3
0 supplicant-timeout 30 server-timeout 30 max-request 2

Vlan Info:

vlan create 10 name "production" type port
vlan create 11 name "guest" type port
vlan create 12 name "quarantine" type port

! *** EAP ***
!
eapol enable
interface FastEthernet ALL
eapol port 1-2 status auto traffic-control in-out re-
      authentication enable re-authentication-period 3600 re-
      authenticate quiet-interval 60 transmit-interval 3 0
      supplicant-timeout 30 server-timeout 30 max-request 2


! *** Port Mirroring ***
!
port-mirroring mode XrxOrXtx monitor-port 9 mirror-port-X 12
!
```

12

Reports

Chapter Contents

Report Types 12-2
Generating Reports 12-4
Viewing Report Details 12-6
Printing Reports 12-7
Saving Reports to a File 12-8
Converting an HTML Report to a Word Document 12-9

Report Types

NAC 800 generates the following types of reports:

Report	Description	Report columns
NAC policy results	Lists each NAC policy and the last pass/fail policy results	• policy name • test status • # of times • % of total • details
Endpoint list	Lists each endpoint and the last pass/fail policy results	• mac address • ip address • cluster • netbios • user • test status
Test details	Comprehensive list of all test results, including remediation messages.	• date/time • ip address • netbios • user • policy • test name • actions • test status • message
Test results	Lists each test and the test's pass/ fail status.	• test name • test status • # of times • % of total • details
Test results by IP address	Lists the number of tests that passed or failed for each IP address.	• ip address • cluster • netbios • user • test status • # of times • % of total • details

Table 12-1.Report Types and Fields

Report	Description	Report columns
Test results by NetBIOS name	Lists the number of tests that passed or failed for each netbios name.	• netbios • cluster • ip address • user • test status • # of times • % of total • details
Test results by user	Lists the number of tests that passed or failed for each user.	• user • cluster • ip address • netbios • test status • # of times • % of total • details

Table 12-1.Report Types and Fields (cont.)

TIP: Click the underlined links in reports for more information about the tests.

Sort the report by clicking the report column heading.

Generating Reports

To generate a report:

NAC 800 Home window>>Reports

The following figure shows the **Reports** window.

Figure 12-1. Reports Window

1. In the **Report** drop-down list, select the report to run.
2. Select the **Report period**.
3. Select the **Rows per page**.
4. In the **Endpoint search criteria** area, select any of the following options to use for filtering the report:
   a. Cluster
   b. Endpoint NetBIOS
   c. Endpoint IP address
   d. Endpoint MAC address
   e. Endpoint test status
   f. Access control status
   g. Endpoints must match:
      i. All of the selected criteria

ii. Any of the selected criteria

5. Select **Generate report**. After a short period of time the compiled report is displayed in a separate browser window. The following figure shows an example report.

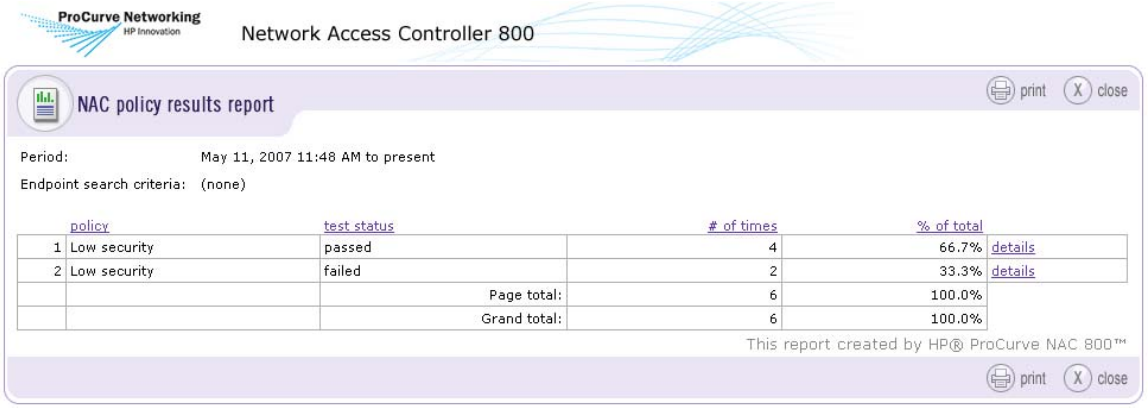


Figure 12-2. NAC Policy Results Report

CAUTION: The reports capability uses pop-up windows; if you have blocked pop-up windows in your browser, you will not be able to view reports. See “Pop-up Windows” on page B-2 for more information.

Viewing Report Details

To view report details:

NAC 800 Home window>>Reports

1. Select the options for the report you want to run.
2. Click **Generate report**.
3. Click the **details** link. The **Test details** window appears:

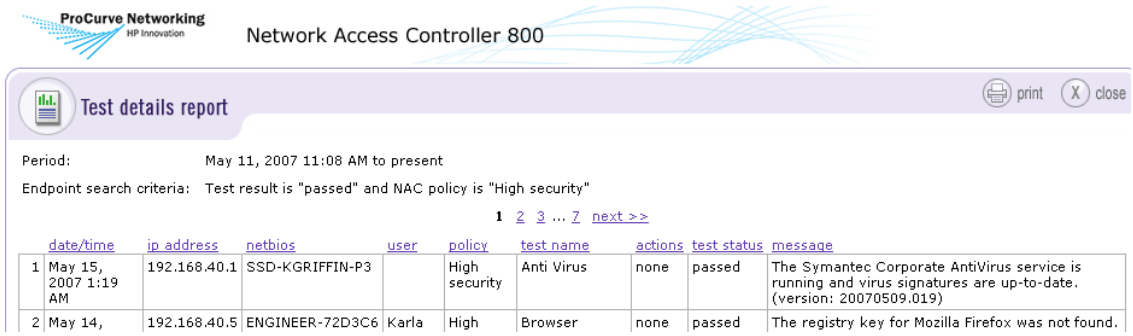

ProCurve Networking
HP Innovation
Network Access Controller 800
Test details report
print
close
Period: May 11, 2007 11:08 AM to present
Endpoint search criteria: Test result is "passed" and NAC policy is "High security"
1 2 3 ... 7 next >>
date/time ip address netbios user policy test name actions test status message
1 May 15, 2007 1:19 AM 192.168.40.1 SSD-KGRIFFIN-P3 High security Anti Virus none passed The Symantec Corporate AntiVirus service is running and virus signatures are up-to-date. (version: 20070509.019)
2 May 14, 192.168.40.5 ENGINEER-72D3C6 Karla High Browser none passed The registry key for Mozilla Firefox was not found.

Figure 12-3. Report, Test Details Window

Printing Reports

To print a report:

NAC 800 Home window>>Reports

1. Select the options for the report you want to run.
2. Click **Generate report**.
3. Select **Print**.
4. Select the printer options and properties.
5. Select **Print**.

Saving Reports to a File

To save a report:

NAC 800 Home window>>Reports

1. Select the options for the report you want to run.
2. Click **Generate report**.
3. Select **File>>Save Page As** from the browser menu.
4. Enter a name and location where you want to save the file.
5. Select **Web page, complete**.
6. Click **Save**. The file is saved as an HTML file that can be viewed in a browser window.

Converting an HTML Report to a Word Document

To convert an HTML report:

1. Run the report (see “Generating Reports” on page 12-4.)
2. Save an HTML version of it (see “Saving Reports to a File” on page 12-8).
3. Open the HTML report in Microsoft Word.
4. Select **File>>Save as**.
5. In the **Save as type** drop-down list, select **.doc**.
6. Click **Save**.
   This creates a standalone file that retains all of its graphics and formatting.
7. To print, you might need to reduce the border sizes in **File>>Page Setup** dialog box for the report to print correctly.

(This page intentionally left blank.)

13

System Administration

Chapter Contents

Launching NAC 800 13-3
- Launching and Logging into NAC 800 13-3
- Logging out of NAC 800 13-3
- Important Browser Settings 13-3

Downloading New Tests 13-4

System Settings 13-5
- Matching Windows Domain Policies to NAC Policies 13-5
- Setting the Access Mode 13-5
- Naming your Enforcement Cluster 13-6
- Changing the MS Host Name 13-6
- Changing the ES Host Name 13-6
- Resetting your System 13-6
- Changing Properties 13-7
- Specifying an Email Server for Sending Notifications 13-8
- Windows 2003 Server Settings 13-8

Entering Networks Using CIDR Format 13-9

Database 13-10
- Creating a Backup File 13-10
- Restoring from Backup 13-10
- Restoring the Original Database 13-11
- Generating a Support Package 13-11

Supported VPNs 13-12

Adding Custom Tests 13-13
- Introduction 13-13
- References 13-13
- Changing the Error Messages in a Test Script 13-13
- Creating a Custom Test Class Script from Scratch 13-18
- BasicTests API 13-28

End-user Access Windows 13-33

How NAC 800 Handles Static IP Addresses 13-34

Managing Passwords 13-35
- Resetting the NAC 800 Server Password 13-36

Resetting the NAC 800 Database Password 13-37
Changing the NAC 800 Administrator Password 13-37
Working with Ranges 13-39
Creating and Replacing SSL Certificates 13-41
Creating a New Self-signed Certificate 13-42
Using an SSL Certificate from a known Certificate Authority (CA) . . . 13-43

Launching NAC 800

Launching and Logging into NAC 800

To launch and log into NAC 800:

Browser window on the workstation

1. Using `https://`, point your browser to the NAC 800 Management Server (MS) IP address or host name. The login page appears.
2. Enter the **User name** and **Password** that you defined the first time you logged in.
3. Click **log in**. The NAC 800 **Home** window appears.

Logging out of NAC 800

To log out of NAC 800:

Any NAC 800 window

Click **Logout** in the upper right corner of the NAC 800 home window. When the logout procedure completes, the ProCurve login window appears.

Important Browser Settings

There are several browser configuration settings to make, depending on which browser you are using. Please see “Important Browser Settings” on page B-1 for details.

Downloading New Tests

To download the latest tests from the ProCurve server:

NAC 800 Home window>>System configuration>>Test updates>>Check for test updates button

TIP: If you are not receiving test updates, try the following checks:
- Verify that the system time is correct
- Attempt to connect using telnet:
  At a command prompt on the MS, enter:
  telnet update.hp.com 443

If you do not get a “connected” response, the firewall might be blocking the traffic.

NOTE: Your outbound SSL connection needs to access:

For license validation and test updates:
update.hp.com port 443

For software and operating system updates
download.hp.com (216.183.121.206) port 80

System Settings

Matching Windows Domain Policies to NAC Policies

Using a Windows domain might affect the end-user's ability to change their system configuration to pass the tests. For example, in a corporate environment, each machine gets their domain information from the domain controller, and the user is not allowed to change any of the related settings, such as receiving automatic updates and other IE security settings.

The NAC 800 administrator needs to make sure the global policy on their network matches the NAC policy defined, or skip the test.

For example, if the global network policy is to not allow Windows automatic updates, any user attempting to connect through the **High security** NAC policy fails the test, and is not able to change their endpoint settings to pass the test. In this example, change the NAC policy to not run the Windows automatic update test:

NAC 800 Home window>>NAC policies

1. Select the NAC policy that tests the domain's endpoints.
2. Select the **Tests** menu option.
3. Clear the **Windows automatic updates** check box.
4. Click **ok**.

Setting the Access Mode

The access mode selection is a quick way to shut down all traffic into an Enforcement cluster, or open it up for trial-use purposes.

To change the access mode:

NAC 800 Home window>>System monitor>>Select an Enforcement cluster

1. Select one of the following from the **Access mode** area:
   - **normal** – Access is regulated by the NAC policies
   - **allow all** – All requests for access are granted, but endpoints are still tested

- **quarantine all** – No access is granted, but endpoints are still tested

2. Click **ok**.

Naming your Enforcement Cluster

To name your Enforcement cluster:

NAC 800 Home window>>System configuration>>Enforcement clusters & servers>>Select an Enforcement cluster

1. In the **Cluster name** text field, enter a name. Choose a name that describes the cluster, such as a geographic location (like a street or city name), a building, or your company name.
2. Click **ok**.

Changing the MS Host Name

To change the MS host name:

See “Modifying Management Server Network Settings” on page 3-23.

Changing the ES Host Name

To change the ES host name:

See “Changing the Enforcement Server Network Settings” on page 3-17.

Resetting your System

To reset your system to the as-shipped state:

Command line window

1. Log in as `root` to the NAC 800 MS, either using SSH or directly with a keyboard.
2. Enter the following command at the command line:

   ```
   resetSystem.py [both | ms | es]
   ```

   Where:

No arguments – The system is reset to the same type (either a single-server installation with the MS and ES on the same server, an MS, or an ES), the database is cleared, and the property files are restored to their defaults

`ms` – The system is reset to be an MS, the database is cleared, and the property files are restored to their defaults

`es` – The system is reset to be an ES, the database is cleared, and the property files are restored to their defaults.

TIP: See the installation guide for instructions on resetting the system using the LCD panel.

NOTE: The resetSystem.py file is in the following directory:

```
cd /usr/local/nac/bin
```

Changing Properties

To change the property values in the properties files:

Command line window

1. Log in as `root` to the NAC 800 MS using SSH.
2. Enter the following at the command line:

   `setProperty.py` <*DESTINATION*> <*TYPE*> <*VALUES*>

   Where:

   - <*DESTINATION*> is one or more of:

     `-c` <*cluster name*> Set properties on all Enforcement Servers in cluster
     `-e` <*ES hostname*> Set properties on Enforcement Server
     `-a` Set properties on all Enforcement Servers
     `-m` Set properties on Management Server
   - <*TYPE*> is
     blank, nothing specified
     `-l` Properties are log4j properties

- <*VALUES*> is one of:
  `-f` <*filename*> Filename of lines containing key=value
  `-` Standard input containing key=value
  <*key*>=<*value*> One or more key=value settings
  Note: a <*value*> of `'-'` will delete the property

Specifying an Email Server for Sending Notifications

NAC 800 Enforcement clusters send alerts and notifications when certain events occur. You must specify an SMTP email server for sending these notifications. The server must allow SMTP messages from the NAC 800 Enforcement server.

To specify an email server for sending notifications:

See “Notifications” on page 3-102.

Windows 2003 Server Settings

Windows 2003 Server has the **Enhanced Security Configuration** option **Enabled** by default. This option must be disabled for the following reasons:

- A Windows 2003 Server host cannot be tested.
- The Windows 2003 Server endpoint cannot download the agent.

To disable the Enhanced Security Configuration option:

Start>>Settings>>Control panel>>Add/Remove Programs>>Add/Remove Windows Components

Clear the selected **Enhanced Security Configuration** option.

TIP: Alternatively, you could select the NAC 800 MS and ES IP addresses as trusted sites.

Entering Networks Using CIDR Format

Networks and network endpoints can be specified in NAC 800 using Classless Inter Domain Routing (CIDR) format. CIDR is a commonly used method for specifying Internet objects. table 13-1 presents common CIDR naming conventions.

Block	Netmask	Networks	Hosts
/32	255.255.255.255	1/256 of a Class C Network	1
/31	255.255.255.254	1/128	2
/30	255.255.255.252	1/64	4
/29	255.255.255.248	1/32	8
/28	255.255.255.240	1/16	16
/27	255.255.255.224	1/8	32
/26	255.255.255.192	1/4	64
/25	255.255.255.128	1/2	128
/24	255.255.255.0	1 Class C network	256
/23	255.255.254.0	2 Class C networks	512
/22	255.255.252.0	4 Class C networks	1,024
/21	255.255.248.0	8 Class C networks	2,048
/20	255.255.240.0	16 Class C networks	4,096
/19	255.255.224.0	32 Class C networks	8,192
/18	255.255.192.0	64 Class C networks	16,384
/17	255.255.128.0	128 Class C networks	32,768
/16	255.255.0.0	1 Class B network	65,536
/15	255.254.0.0	2 Class B networks	131,072
/14	255.252.0.0	3 Class B networks	262,144
/13	255.248.0.0	8 Class B networks	512,000

Table 13-1.CIDR Naming Conventions

Database

Creating a Backup File

To create a backup file of system configuration and data:

See “Initiating a New Backup” on page 3-91.

Restoring from Backup

To restore system configuration and data from a backup file:

NOTE: You must have backed up your system at least one time before you can restore from a backup.

NAC 800 Home window>>System configuration>>Maintenance

1. Click **restore system from backup** file. The **Restore system** window appears:

Figure 13-1. Restore System Window

2. Enter the backup file name or click **Browse** and navigate to the backup file.
3. Click **ok**. A status window appears.

4. The system data is restored and the login window appears:

Figure 13-2. Login Window

Restoring the Original Database

CAUTION: Running this script resets your entire system, not just the database. See "Resetting your System" on page 13-6 for more information.

To reset a NAC 800 database to its pristine state:

Command window

1. Log in as **root** to the NAC 800 MS using SSH.
2. Enter the following commands:

   ```
   resetSystem.py
   ```

   This script shuts down all of the services, cleans the database, iptables, and DHCP server, and restarts everything.

Generating a Support Package

To generate a support package:

See "Downloading Support Packages" on page 3-94.

Supported VPNs

NAC 800 works with any VPN endpoint, since NAC 800 does not directly interface or inter-operate with VPN endpoints. The following commonly deployed VPN solutions have been tested:

- Cisco VPN: 30xx series
- Microsoft 2000 and 2003 Server (VPN capability enabled)
- OpenVPN
- Protocols supported:
  - IPSec
  - L2TP
  - PPTP
  - SSL

Adding Custom Tests

Introduction

NAC 800 is an efficient, flexible and extensible testing platform. All tests are implemented in the object oriented programming language called Python. Python is a well- respected, *clean*, and efficient scripting language. Because the language is object oriented and the NAC 800 test platform is extensible, new tests can be developed easily.

Existing tests can also be extended using inheritance—a programming language's ability to derive one class/script from another class and override and extend methods of that class.

You need some programming experience to extend and add tests. If you have previously used Perl to complete these tasks, you might find that Python is a better choice as a programming language for the tasks described in the following sections.

CAUTION: You should familiarize yourself with Python and with the rest of the NAC 800 product before attempting to create custom test scripts.

References

This version of NAC 800 uses Python v2.4.1.

- Python home:
  http://www.python.org/
- Python 2.4.1 tutorial:
  http://www.python.org/doc/2.4.1/tut/tut.html
- Python language reference:
  http://www.python.org/doc/2.4.1/

Sample test scripts are on the NAC 800 CD in the `/sampleTests` folder.

Changing the Error Messages in a Test Script

Using Python, try changing the error messages in an existing test script. This task can help you to familiarize yourself with the NAC 800 scripting API. Each NAC 800 test script defines a test class. To change an error message, create a new script that derives a new test class from an existing test class and modify the return hash of the `runTest` method. For example:

1. Log in as `root` to the NAC 800 server using SSH.
2. Open the `/sampleTests/myCheckSoftwareNotAllowed.py` file on the NAC 800 CD in a text editor.
3. Examine the code. The comments explain each section of code. The following example shows the contents of the file.

```
#!/usr/bin/python
from checkSoftwareNotAllowed import CheckSoftwareNotAllowed

#
# This allows a script to be tested from the command line.
#
if __name__ == '__main__':

    import myCheckSoftwareNotAllowed
    t = myCheckSoftwareNotAllowed.MyCheckSoftwareNotAllowed()
    t.processCommandLine()

#
# The class definition. MyCheckSofwareNotAllowed is derived
# from the existing test CheckSoftwareNotAllowed and inherits
# all the existing tests functionality.
#
class MyCheckSoftwareNotAllowed(CheckSoftwareNotAllowed):




    #
    # Override the testId to be unique from all other test ids
    #
    testId = "MyCheckSoftwareNotAllowed"

    #
    # Rename your derived test
    #
    testName = "My check software not allowed"
```

Figure 13-3. Test Script Code

```
#
# All test classes must define the runTest method with the self and debug
# parameters
#
def runTest(self,debug=0):

    #
    # Get the result hash from the CheckSoftwareNotAllowed test
    # and modify the result message based on the result code.
    #
    result = CheckSoftwareNotAllowed.runTest(self,debug)
    if result["result_code"] == "fail":
        result["result_message"] = "The MyCheckSoftwareNotAllowed test
  failed."
    elif result["result_code"] == "pass":
        result["result_message"] = "The MyCheckSoftwareNotAllowed test
  passed."


    return result
```

Figure 13-3. Test Script Code (cont.)

4. You can change the `result["result_message"]` to whatever text you want. This message is what the end-user sees in the access windows. This text also appears in the management console when you run reports.
5. Every test must return a hash with the following keys:

   ```
   status_code - 0 test did not run, error occurred, 1
   test ran
   result_code - pass, fail
   result_message - the text to display to the user
   ```

NOTE: Do not change the status_code or the result_code for this example.

6. Once you have completed your edits and saved the `myCheckSoftwareNotAllowed.py` file, copy it to the following directory on the NAC 800 MS:

   ```
   /usr/local/nac/scripts/Custom/Tests
   ```

7. If you have created new base classes, copy them to the following directory on the NAC 800 MS:

   ```
   /usr/local/nac/scripts/Custom/BaseClasses
   ```

CAUTION: When updating or modifying files, use the Custom directory tree (Custom/BaseClasses, Custom/Tests). The Custom directory tree is a mirror (with symbolic links) to the live test tree (scripts/BaseClasses and scripts/Tests). The live tree is not modified directly, but is modified with the installCustomTests script and the RPM mechanism.

8. Once your custom test script is complete, and you are ready to push it out to all of the ESs, verify that the scripts and base classes are under the Custom directory tree as specified above, and enter the following on the command line of the NAC 800 MS:

   ```
   installCustomTests
   ```

   This command compiles the Python source files, builds an RPM, updates the policy groups, and sends these changes to *all* ESs. An example of the output from the `installCustomTests` command is shown as follows:

NOTE: This command affects all ESs, even those that are not currently up and running. Once a stopped ES comes back up, the ES is updated.

```
# installCustomTests
Creating custom test script RPM version 5.0-51
Found 5 python files
 + Compiling python scripts
 + Generating test script XML files

If you continue, this will generate an RPM file containing your custom scripts
and will send the new custom script RPM to the Management Server and all
Enforcement Servers.


--> Press Enter to proceed or Ctrl-C to abort <--
 + Generating RPM spec file
 + Creating RPM file 'NAC-custom-testscripts-5.0-51.i386.rpm'
 + Creating update package file (/tmp/customUpdatePkg.29285.tar.gz)
 + Creating XML file to send custom scripts to the MS (/tmp/
      installCustomTest.29285.xml)
 + Sending XML message to MS to install and distribute custom scripts
00:22:34 INFO  channel status changed: Channel: TcpTransportChannel:
      Socket[addr=localhost/127.0.0.1,port=61616,localport=44041] has connected
```

Figure 13-4. Example InstallCustomTests Output

```
00:22:34 DEBUG TCP consumer thread starting
00:22:34 DEBUG Created temporary queue: TemporaryQueue-{TD{ID:perf-ms1-40612-
      1162365754580-1:0}TD}ID:perf-ms1-40612-1162365754580-6:0
00:22:34 DEBUG Sending request:
<UpdateRequest>
  <requestParameters>
    <entry>
      <string>UPDATE_DATA</string>
      <string>/tmp/customUpdatePkg.29285.tar.gz</string>
    </entry>
  </requestParameters>
</UpdateRequest>

00:22:34 DEBUG Sending message: ACTIVEMQ_TEXT_MESSAGE: id = 0 ActiveMQMessage{
      , jmsMessageID = ID:perf-ms1-40612-1162365754580-7:0, bodyAsBytes =
      org.activemq.io.util.ByteArray@1112783, readOnlyMessage = false,
      jmsClientID = 'ID:perf-ms1-40612-1162365754580-1:0' , jmsCorrelationID =
      'null' , jmsDestination = nac.requests, jmsReplyTo = TemporaryQueue-
      {TD{ID:perf-ms1-40612-1162365754580-1:0}TD}ID:perf-ms1-40612-
      1162365754580-6:0, jmsDeliveryMode = 2, jmsRedelivered = false, jmsType =
      'null' , jmsExpiration = 1162365784872, jmsPriority = 4, jmsTimestamp =
      1162365754872, properties = null, readOnlyProperties = false,
      entryBrokerName = 'null' , entryClusterName = 'null' , consumerNos =
      null, transactionId = 'null' , xaTransacted = false, consumerIdentifer =
      'null' , messageConsumed = false, transientConsumed = false,
      sequenceNumber = 0, deliveryCount = 1, dispatchedFromDLQ = false,
      messageAcknowledge = null, jmsMessageIdentity = null, producerKey =
      ID:perf-ms1-40612-1162365754580-7: }, text = <UpdateRequest>

<requestParameters>
    <entry>
      <string>UPDATE_DATA</string>
      <string>/tmp/customUpdatePkg.29285.tar.gz</string>
    </entry>
  </requestParameters>
</UpdateRequest>


00:22:34 DEBUG Waiting for a response on :TemporaryQueue-{TD{ID:perf-ms1-40612-
      1162365754580-1:0}TD}ID:perf-ms1-40612-1162365754580-6:0
```

Figure 13-4. Example InstallCustomTests Output (cont.)

```
00:22:36 DEBUG Message received: ACTIVEMQ_TEXT_MESSAGE: id = 0 ActiveMQMessage{
      , jmsMessageID = ID:perf-ms1-51331-1162363440379-15:3, bodyAsBytes =
      org.activemq.io.util.ByteArray@1362012, readOnlyMessage = true,
      jmsClientID = '93baaf5a-b0ed-4fc2-a3ae-ec6460caedc0' , jmsCorrelationID =
      'null' , jmsDestination = TemporaryQueue-{TD{ID:perf-ms1-40612-
      1162365754580-1:0}TD}ID:perf-ms1-40612-1162365754580-6:0, jmsReplyTo =
      null, jmsDeliveryMode = 2, jmsRedelivered = false, jmsType = 'null' ,
      jmsExpiration = 1162365766750, jmsPriority = 4, jmsTimestamp =
      1162365756750, properties = null, readOnlyProperties = true,
      entryBrokerName = '172.30.1.50' , entryClusterName = 'default' ,
      consumerNos = [0], transactionId = 'null' , xaTransacted = false,
      consumerIdentifer = 'ID:perf-ms1-40612-1162365754580-1:0.1.1' ,
      messageConsumed = false, transientConsumed = false, sequenceNumber = 3,
      deliveryCount = 1, dispatchedFromDLQ = false, messageAcknowledge =
      org.activemq.ActiveMQSession@73a34b, jmsMessageIdentity = null,
      producerKey = ID:perf-ms1-51331-1162363440379-15: }, text =
      <NACResponse><resultStatus>true</resultStatus><response
      class="string">9X</response><ip>172.30.1.50</ip><id>MNM</
      id><originalTimeStamp>1162365756707</originalTimeStamp></NACResponse>
00:22:36 DEBUG Received: <NACResponse><resultStatus>true</
      resultStatus><response class="string">9X</response><ip>172.30.1.50</
      ip><id>MNM</id><originalTimeStamp>1162365756707</originalTimeStamp></
      NACResponse>

Done
```

Figure 13-4. Example InstallCustomTests Output (cont.)

NOTE: The output between the "+ Sending XML message to MS to install and distribute custom scripts" message and the "Done" message in figure 13-4 is output from the command that installed the custom scripts and shows the status of the sending the XML JMS request to the MS.

Creating a Custom Test Class Script from Scratch

Creating a custom test script is similar to the previous error message example; however, you must define a few more things and then add your own test functionality. Examine the test script template shown in figure 13-5. The comments explain each section of code. Once you are comfortable with the template, the following section contains an example that shows how to create a `checkOpenPorts.py` test script, which tests an endpoint for specified open ports.

TIP: This template file is included on the CD at /sampleTests/testTemplate.py, so you can edit it instead of retyping it.

```
#!/usr/bin/python
from BaseClasses.SABase import SABase as SABase

#
# This allows a script to be tested from the command line.
#
if __name__ == '__main__':

    import testTemplate
    t = testTemplate.TestTemplate()
    t.processCommandLine()



#
# The class definition. All classes must be derived from the SABase class.
#
class TestTemplate(SABase):

    #
    # Make up a test id. Just make sure it doesn't match any existing test
      ids.
    #
    testId = "TestId"

    #
    # Make up test name. Just make sure it doesn't match any existing test
      names.
    #
    testName = "Test Name"
```

Figure 13-5. testTemplate.py

```
#
# Assign the test to an existing group or create a new group.
# Groups are configured and created in the policies.xml file <group>
# section (See the Adding new groups section).
#
testGroupId = "TestGroup"

#
# This is the HTML that will be displayed in the test properties page
# in the policy editor.
#
testConfig = \
"""
<HTML>Test Config HTML</HTML>
"""

#
# These are any default values you want to assign to the input parameters
# in the testConfig HTML.
#
defaultConfigValues = {}


#
# A short summary for the test.  This will show up in the description
  field
# when editing NAC policies in the management UI.
#
testSummary = \
"""
My short description
"""


#
#
# This is field is unused at the moment.
# field in the policy editor.
#
testDescription = ''


#
# These are the arguments to run the test. This is displayed in the
  command
# line help.
#
testArguments = \
"""
My test arguments
"""
```

Figure 13-5. testTemplate.py (cont.)

```
#
# All tests must define the runTest method with the self and the debug
# parameters.
#
def runTest(self,debug=0):

   #
   # All tests must call the initialize routine
   #
   self.initTest()



   #
   # Create a hash to store the return results.
   # All tests must fill return a hash with the following keys:
   #
   #     status_code    - 0 if an unexpected error occurred, 1 if
  successful
   #     result_code    - pass, fail or some error
   #     result_message - the message to display to the end-user
   #
   returnHash = {}
   returnHash["status_code"] = 1
   returnHash["result_code"] = "pass"
   returnHash["result_message"] = "Some nice text that a user can read
  here."


   try:

       #
       # Replace 'pass' with your test here. Modify the returnHash
  accordingly.
       #
       pass


   except:
       #
       # Set the return status when exception occurs
       #
       import sys
       returnHash['status_code'] = 0
       returnHash['result_code'] = "unknown_error"
       returnHash['result_message']  = sys.exc_type, sys.exc_value
       return(returnHash)
```

Figure 13-5. testTemplate.py (cont.)

```
 #
 # Always use the doReturn function; this allows superclass to add or
modify
 # any items in the returnHash as necessary.
 #
 return(self.doReturn(returnHash))
```

Figure 13-5. testTemplate.py (cont.)

1. Use the template, as shown in figure 13-5, to create a new test script. As an example, the new test script is called `checkOpenPorts.py`, and it fails if any of the specified ports are open on the target host being tested. Before examining the code, consider the following information about the test scripts:
   - All test scripts contain a `self.inputParams` hash table that has all input parameters configured through the policy properties HTML. For example, if the `testConfig` variable for the test is set to:

     ```
     <input id="myparam" name="myparam" value="">
     ```

     Then, the self `inputParams` contains a `myparams` key that is set to the value of the HTML input element set in the policy editor.
   - All test scripts contain a `self.session` member variable that is set by NAC 800 when the test class is instantiated. It contains a reference to a Session object, which is a built-in Python class defined by NAC 800 and is used internally by the `BasicTests` class described later in this section. However, to retrieve the host name or IP address, use `host()` method:

     ```
     self.session.host()
     ```

     when developing scripts.
   - All tests contain a reference to the `BasicTests` class called `self.bt`. The `self.bt` class gives you access to commonly used functions for testing endpoints including registry operations and service operations. See “BasicTests API” on page 13-28 for more information on the `BasicTests` API. This example does not use this API.

2. figure 13-6 shows the code for the new `checkOpenPorts.py` test. The file is included on the NAC 800 CD as `/sampleTests/checkOpenPorts.py`. Review the code. The comments explain each section of the code.

```
#!/usr/bin/python
from BaseClasses.SABase import SABase as SABase

#
# This allows a script to be tested from the command line.
#
if __name__ == '__main__':

    import checkOpenPorts
    t = checkOpenPorts.CheckOpenPorts()
    t.processCommandLine()



#
# The class definition. All classes must be derived from the SABase class.
#
class CheckOpenPorts(SABase):

    #
    # Make up a test id. Just make sure it doesn't match any existing test ids
    #
    testId = "CheckOpenPorts"

    #
    # Make up test name. Just make sure it doesn't match any existing test
      names.
    #
    testName = "Open ports"


    #
    # Assign the test to an existing group or create a new group.
    # Groups are configured and created in the policies.xml file <group>
    # section (See the Adding new groups section).
    #
    testGroupId = "MyCustomTests"

    #
    # This is the HTML that will be displayed in the test properties page
    # in the policy editor. All this HTML isn't REALLY necessary, but we
    # to keep the NAC 800 Web UI pretty.
    #
```

Figure 13-6. checkOpenPorts.py script

```
testConfig = \
"""
<div id="test_parameters">
    <table height="100%" width="100%" border="0" cellspacing="0"
  cellpadding="0">
    <tbody>
        <tr>
            <td colspan="2" style="padding: 5px 3px 5px 3px;">
            Enter a list of ports that are not allowed to be open on the
            endpoint. Add ports separated by a comma. For example, 23,80.
            </td>
        </tr>
        <tr>
            <td style="padding: 3px 0px 3px 3px;">
                <textarea name="ports_not_allowed" rows="5" cols="30"
  wrap="on" style="border: 1px solid #A894D1;
                    font-family: Arial, Helvetica, sans-serif; font-size:
  8pt; padding: 1px 2px 1px 2px;"></textarea>
            </td>
        </tr>
    </tbody>
    </table>
</div>
"""


#
# These are any default values you want to assign to the input parameters
# in the testConfig HTML. The first time this test is configured for a
# policy or if the test is never configured for a policy, this will be
# the default. Notice the key in this hash corresponds to the input
  element
# above in the testConfig.
#
defaultConfigValues = { "ports_not_allowed" : "23,80" }


#
# Make up a detailed description for the test.
#
testDescription = \
"""
This test takes a list of ports that should NOT be found open on
the remote host.  If any port is found open, this test will
fail.  This script will only succeed if none of the undesired ports
are found open.
"""
```

Figure 13-6. checkOpenPorts.py script (cont.)

```
#
# Make up a summary for the test. This will show up in the description
# field in the policy editor.
#
testSummary = "This test takes a list of ports that should NOT be found
  open on the remote host. If any port is found open, this test will fail.
  This script will only succeed if none of the undesired ports are found
  open."


#
# These are the arguments to run the test. This is displayed in the
  command
# line help.
#
testArguments = \
"""
--host=<hostname, IP, or NETBIOS>
--input ports_not_allowed=<comma delimited list of ports>


Example: <this script> --host=somehost --input
  "ports_not_allowed=23,80"
"""

#
# All tests must define the runTest method with the self and the debug
# parameters.
#
def runTest(self,debug=0):

    #
    # All tests must call the initialize routine
    #
    self.initTest()

    if debug:
        print "Starting checkOpenPorts(host="+self.session.host()+",
  session="+self.session.id()+")"


    #
    # Create a hash to store the return results.
    # All tests must fill return a hash with the following keys:
    #
    #     status_code    - 0 if an unexpected error occurred, 1 if
  successful
    #     result_code    - pass, fail or some error
    #     result_message - the message to display to the end-user
    #
    returnHash = {}
    returnHash["status_code"] = 1
    returnHash["result_code"] = "pass"
    returnHash["result_message"] = "The ports were not open."
```

Figure 13-6. checkOpenPorts.py script (cont.)

```
    try:
        ports = []
        if self.inputParams.has_key("ports_not_allowed"):
            ports = self.inputParams["ports_not_allowed"].split(",")
        else:
            # No ports not allowed, pass
            return(self.doReturn(returnHash))


        if debug:
            print "Checking ports " + str(ports) + " on host " +
self.session.host()

        #
        # Do your test here. Modify the returnHash accordingly.
        #
        portsOpen = ""

        #
        # Use a Python socket to connect directly to the target host
        #
        import socket



        for p in ports:

            hp = self.session.host()+":"+str(p)
            s = None
            try:
                if debug:
                    print "Connecting to " + hp



                #
                # Try to open the port. Throws an exception if connection
                # is refused or times out (set timeout to 5 seconds).
                #
                # Note that NAC 800 uses a restricted Python socket
                # library that doesn't allow connections to arbitrary
                # hosts.  Normally, the first element of the tuple passed
                # to socket.connect() is the IP or hostname; in SA, you
                # must pass the Session object form which the socket
                # object will get the target host IP/name.
                #
                s = socket.socket()
                s.settimeout(5)
                s.connect((self.session, int(p)))

                # Uh oh, no exception. The port was open
```

Figure 13-6. checkOpenPorts.py script (cont.)

```
                s.close()

                if debug:
                    print "Connected to "+hp+". Port open!"

                #
                # Add the port to our list of open ports for use later
                #
                portsOpen += str(p) + ","
            except:
                if s is not None:
                    try:
                        s.close()
                    except:
                        pass


                import sys
                print "checkOpenPorts(host="+self.session.host()+",
session="+self.session.id()+"): ", sys.exc_type, sys.exc_value
                if debug:
                    print "Could not connect to "+hp+". Port not open."
                # Good, it wasn't open

        #
        # There are ports open, so set the returnHash values
        # to indicate that the endpoint failed the test.
        #
        if portsOpen != "":
            returnHash["status_code"] = 1
            returnHash["result_code"] = "fail"
            returnHash["result_message"] = "The following ports that are
not allowed open were open: " + portsOpen.rstrip(", ")



    except:
        #
        # Set the return status when exception occurs
        #
        import sys
        returnHash['status_code'] = 0
        returnHash['result_code'] = "unknown_error"
        returnHash['result_message'] = sys.exc_type, sys.exc_value
        return(returnHash)

    #
    # Always use the doReturn function. This will record test timings as
well as
    # encode the result_message into a format compatible with NAC 800
    #
    return(self.doReturn(returnHash))
```

Figure 13-6. checkOpenPorts.py script (cont.)

3. Once you have completed your test script modifications, save the script as described in step 6 on page 13-15.

4. Save any new classes as described in step 7 on page 13-15.
5. Push the new test out to all ESs as described in step 8 on page 13-16.
6. For the final test, connect to:

   ```
   http://<NAC 800 ip>:88
   ```

   and test your Windows endpoint. If you have ports open that are not allowed, this test fails.

BasicTests API

Every NAC 800 test has a base functionality described as follows:

```
        …
        try:
                self.bt.getregKeyExists(
"HKEY_LOCAL_MACHINE\\Software\\America Online\\AIM")
                except:
                        import sys
                        returnHash["status_code"] = 0
                        returnHash["result_code"] =
"unknown_error"
                        returnHash["result_message"] =
sys.exc_type, sys.exc_value
        …
```

The following table describes the BasicTests API.

The BasicTests API accesses these functions with the SABase self.bt member. All methods throw an exception that should be caught if an unexpected error occurs.

Return Value	Public Method
Network API	
String	getMacAddresses(debug = 0) Retrieves the MAC addresses for all interfaces on an endpoint. Returns a carriage return separated string. Each line is in the following format: <IP address> <MAC address> <internal transport name> <true if configured for DHCP|false if not>
String	getNetBIOSName(debug=0) Returns the NetBIOS name of the specified host.

Table 13-2.BasicTests API

The BasicTests API accesses these functions with the SABase self.bt member. All methods throw an exception that should be caught if an unexpected error occurs.

Return Value	Public Method
String	getOs(debug=0) Retrieves the operating system of the `targetHost`. Returns one of the following strings: • Windows 98 • Windows ME • Windows NT • Windows 2000 • Windows XP • Windows Server 2003 • Unknown
String	dhcpRelease(debug=0) Forces a DHCP release of the specified host.
String	dhcpRenew(debug=0) Forces a DHCP release and renew of the specified host.

Service API

The serviceName parameters can be the registry name or the display name. For example, TIntSvr or Telnet can be used to identify the Telnet service.

For performance reasons, it is important to use the same case when specifying the same service name in multiple calls. Even though the windows process table is not case-sensitive, the test result cache is case-sensitive.

Boolean	getServiceExists(string serviceName, debug=0) Check to see if a service is installed. Returns the following: • 1 if exists • 0 if it doesn't exist
Int	getServiceSetting(string serviceName, debug=0) Check to see if a service is set to auto, manual, or disabled. Returns one of the following integers: • 0 if auto • 1 if manual • 2 if disabled

Table 13-2.BasicTests API (cont.)

The BasicTests API accesses these functions with the SABase self.bt member. All methods throw an exception that should be caught if an unexpected error occurs.

Return Value	Public Method
String	getServiceStatus(list serviceNames, debug=0) Gets the status for a list of services. Returns a hash containing the `result_data` key. The value of this key is a hash with a key for each service in the serviceNames. The value of the service hash is one of the following strings: • Stopped • Running • Paused • Not Installed
Nothing	startService(serviceName,debug=0) Starts the service serviceName if it is stopped or paused.
Nothing	stopService(serviceName,debug=0) Stops the service serviceName if it is started or paused.

Registry API

Registry key parameters use HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER, HKEY_USER to specify the subtree of the registry. For example, HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion.

For performance reasons, it is important to use the same case when specifying the same registry key in multiple calls. Even though the windows registry is not case-sensitive, the test result cache is case-sensitive.

Dict	getRegEnumKeys(string key, debug=0 Returns a hash containing the `result_data` key. The value of this key is a list of subkeys under key.
Dict	getRegEnumValues(string key, debug=0) Returns a hash containing the `result_data` key. The value of this key is a list of values under key.
String	getRegQueryValue(string key, string value, debug=0) Returns the data associated with the value as a string.
Boolean	getRegValueExists(string key, string value, debug=0) Check to see if a value exists in the registry. Returns the following: • 1 if exists • 0 if it does not exist

Table 13-2.BasicTests API (cont.)

The BasicTests API accesses these functions with the SABase self.bt member. All methods throw an exception that should be caught if an unexpected error occurs.

Return Value	Public Method
Boolean	getRegKeyExists(string key, debug=0) Check to see if a single key exists in the registry. Returns the following: • 1 if exists • 0 if it does not exist
Boolean	getRegValueDataExpression(string key, string expression, debug=0) Check if a value's data matches an expression. Expression is of the format similar to Perl regular expressions. Returns: • 1 if match • 0 if no match
File API	
NOTE: Environment variable templates can be used in filenames. For example, `%AppData%\\Adobe`. For performance reasons, it is important to use the same case when specifying the same file name in multiple calls. Even though the windows file system is not case-sensitive, the test result cache is case-sensitive.	
Int	getFileLastModified(string file, debug=0) Returns: seconds since January 1, 1970
Int	getFileCreated(string file, debug=0) Returns: seconds since January 1, 1970
Boolean	getFileExists(string file, debug=0) Returns the following: • 1 if true • 0 if no false
Boolean	getFileCanRead(string file, debug=0) Returns the following: • 1 if true • 0 if no false
Boolean	getFileCanWrite(string file, debug=0) Returns the following: • 1 if true • 0 if no false

Table 13-2.BasicTests API (cont.)

The BasicTests API accesses these functions with the SABase self.bt member. All methods throw an exception that should be caught if an unexpected error occurs.

Return Value	Public Method
Boolean	getFileIsDirectory(string file, debug=0) Returns the following: • 1 if true • 0 if no false
Boolean	getFileIsFile(string file, debug=0) Returns the following: • 1 if true • 0 if no false
Boolean	getFileIsHidden(string file, debug=0) Returns the following: • 1 if true • 0 if no false
Long	getFileSize(string file, debug=0) Returns the Logical file size in bytes.

Table 13-2.BasicTests API (cont.)

End-user Access Windows

The end-user access windows are completely customizable. You can enter general text through the NAC 800 interface and edit the file that contains the messages that are returned to the end-user.

TIP: If you need more end-user access window customization than is described in this Users' Guide, please contact ProCurve Networking by HP.

Editing the end-user access window logo and general text:

See "End-user Screens" on page 3-104.

Editing the end-user test results message text:

NAC 800 server command line

See "Customizing Error Messages" on page 5-40.

CAUTION: Make changes to the description only. For example, in the following text:

"checkServicePacks.String.3" : "There are no service packs installed. Run Windows Update to install the most recent service packs."

Do not make changes to the text at the beginning of the line: "checkService-Packs.String.3" :

Viewing the end-user access windows:

Open an IE browser window

Point the IE browser to port 88 of your NAC 800 Enforcement server. For example, if the IP address of your NAC 800 Enforcement server is 10.0.16.18, point an IE browser window to:

```
http://10.0.16.18:88
```

TIP: If you would like to use a port other than 88, contact ProCurve Networking by HP for assistance in making the necessary changes.

How NAC 800 Handles Static IP Addresses

The following list details how NAC 800 handles static IP addresses:

- Inline Mode – NAC 800 can detect, test, and quarantine static IP addresses. The end-user cannot circumvent a quarantine.
- DHCP mode
  - NAC 800 can detect and test static IP addresses but cannot quarantine static IP addresses.
  - NAC 800 can detect static IP endpoints in two different ways:
    - Any type of traffic from the endpoint can be detected if that endpoint has any network traffic visible by NAC 800.
  - An endpoint with a static IP address can be automatically tested only if the endpoint:
    - Has credentials stored for agentless testing.
    - Already has the agent installed.

If you do not use the items in the previous list, you cannot capture the users attention in their browser to force them to supply credentials or install an agent and get tested.

  - If an endpoint has a static IP address and it can't be tested automatically, the endpoint shows up as **awaiting test initiation** in the **Endpoint activity** window.
- Any mode – An administrator can manually test any endpoint by pointing the endpoint's browser to **http://<**`NAC 800 Enforcement server IP address>:88.` This includes endpoints with static IP addresses.

Managing Passwords

The passwords associated with your NAC 800 installation are listed in the following table:

NAC 800 password	Set during	Recovery process
NAC 800 Management or Enforcement server	Initial install process *	See "Resetting the NAC 800 Server Password" on page 13-36.
NAC 800 database	Initial install process *	See "Resetting the NAC 800 Database Password" on page 13-37.
NAC 800 console, administrator account	Initial install process *	• For known passwords – NAC 800 Home window >> System configuration >> User accounts • For unknown passwords – See "Changing the NAC 800 Administrator Password" on page 13-37.
endpoint / domain administrator	Manually entered on the endpoint by the end-user. If the end-user has not defined a login/ password combination, the default login is usually "administrator" with a blank password. Known passwords are entered on the System configuration>>Windows>>Agentless credentials window to allow NAC 800 to test the endpoint.	Password recovery on endpoints is beyond the scope of this document.
Windows domain	Manually entered after installation on the System configuration>>Quarantining>>802.1x Quarantine method radio button window.	Windows domain password recovery is beyond the scope of this document.
OpenLDAP	Manually entered after installation on the System configuration>>Quarantining>>802.1x Quarantine method radio button window.	OpenLDAP password recovery is beyond the scope of this document.

* See the *NAC 800 Installation Guide* for the installation process.

Table 13-3.NAC 800 passwords

NAC 800 password	Set during	Recovery process
Novell eDirectory	Manually entered after installation on the System configuration>>Quarantining>>802.1x Quarantine method radio button window.	Novell eDirectory password recovery is beyond the scope of this document.

* See the *NAC 800 Installation Guide* for the installation process.

Table 13-3.NAC 800 passwords

Resetting the NAC 800 Server Password

If you cannot remember the root login password for the NAC 800 MS or ES, use one of the following processes:

- "Serial Console" on page 13-36
- "Reset Appliance Mode" on page 13-37

Serial Console

Connect a serial console (a computer with a terminal emulator) to the NAC 800 appliance's serial connector and perform the following steps:

NOTE: See the installation guide for instructions on connecting a console.

You must set the terminal emulator settings as follows:

9600/8/n/1

To reset the NAC 800 server root password:

1. At the NAC 800 MS or ES server (not through the web or SSH), reboot the MS or ES server by pressing:

   `[CTRL]+[ALT]+[DELETE]`

2. As the machine boots, you are presented with a list of kernels. Interrupt the boot process by pressing the `[a]` key.
3. Press `[e]` to edit the line.
4. Enter a space and type:

   `single`

5. Press `[b]`. You are now in **Single User Mode**.

6. Enter the following command:

   `passwd`

7. Enter a new password at the **New Password** prompt.
8. Press [ENTER].
9. Retype the password at the **Retype new password** prompt.
10. Press [b]. The password is changed.
11. Press [b] to continue booting.

Reset Appliance Mode

On the appliance's LCD, reset the server mode (personality). See the installation guide for instructions on setting and changing the personality.

CAUTION:

Changing the appliance server mode (personality) resets the passwords, but it also restores the entire system to the default state—deleting data and erasing configuration settings.

Resetting the NAC 800 Database Password

The NAC 800 database password is set during the install process. You can not change your database password with NAC 800 later. If your database password gets changed by some other method after NAC 800 is installed, NAC 800 will not be able to communicate with the database. In this case, contact ProCurve Networking by HP for assistance.

Changing the NAC 800 Administrator Password

To reset the NAC 800 administrator console User Name and Password when known:

See "Modifying the MS root Account Password" on page 3-26.

To reset the NAC 800 administrator console User Name and Password when unknown:

Command line window

1. Create a text file with the following lines:

   ```
   Compliance.ObjectManager.AdminUser=
   Compliance.ObjectManager.AdminPassword=
   Compliance.UI.FirstTimeConfigCompleted=true
   ```

   Enter characters following the equal sign that are the password (for example, `CwR0(tW`).

2. Save the file and copy it to the NAC 800 server (either MS or ES).
3. Log into the NAC 800 server as root.
4. Enter the following command:

   `setProperty.py -f<`*filename*`>`

5. From a workstation, open a browser window and point to the NAC 800 Management server.
6. Enter a new **User Name** and **Password** when prompted.

Working with Ranges

In NAC 800 implementations, particularly in trial installations where you are connecting and disconnecting cables to a number of different types of end-points, you can filter the activity by specifying the following:

- Ranges to monitor – This property filters results in the display window, it does *not* keep NAC 800 from testing other systems.
- Ranges to ignore – Does not test the ranges listed.
- Ranges to enforce – This property is only valid for DHCP mode. It modifies the iptables QUEUE rule such that only the networks set to be enforced will ever get quarantine addresses.

To specify ranges to monitor:

NAC 800 home window>>System configuration>>Select an Enforcement Cluster>>Advanced menu option

In the **Endpoint detection** area, enter the range of addresses to monitor in the **IP addresses to monitor** text field. Separate ranges with a hyphen or use CIDR notation.

To specify ranges to ignore:

NAC 800 home window>>System configuration>>Enforcement clusters & servers>>Select an Enforcement Cluster>>Advanced menu option

In the **Endpoint detection** area, enter the range of addresses to ignore in the IP **addresses to ignore** text field. Separate ranges with a hyphen or use CIDR notation.

To specify ranges to enforce:

NAC 800 home window>>System configuration>>Quarantining menu option

1. Select the **DHCP** radio button in the **Quarantine method** area.
2. Select the **Restrict enforcement of DHCP requests to these relay agent IP addresses** radio button.
3. Enter IP addresses in the **DHCP relay IP addresses to enforce** text box. Enter individual DHCP relay agent IP addresses, separated by carriage returns. These addresses must be a subset of either the quarantined or non-quarantined subnets.

NOTE:

When using Extreme switches, **DHCP relay IP addresses to enforce** will NOT work when the quarantine subnet is a subset of the production network. This is because Extreme switches forward the packets from the IP address closest to NAC 800 and not the IP address of the interface closest to the endpoint, so all the DHCPRelay packets will appear to come from a production network IP address.

For example, the following scenario will not work:

NAC 800 IP: 10.241.88.20
Production Network: 10.241.90.0/24
Quarantine Network: 10.241.90.160/27 (161-189 for range)
Gateway IP: 10.241.90.190
Non-Quarantine Network(s): 10.241.90.0/25, 10.241.90.128/27, 10.241.90.192/26

Creating and Replacing SSL Certificates

The Secure Sockets Layer (SSL) protocol uses encryption by way of certificates to provide security for data or information sent over HTTP.

Certificates are digitally signed statements that verify the authenticity of a server for security purposes. They use two keys; one public key to encrypt information and one private key to decipher that information.

`keytool` is a key and certificate management utility that allows you to create your own public and private keys when you use self-authentication. These keys and certificates are stored in a keystore file.

Creating a New Self-signed Certificate

To generate a private keystore containing a new private key/public certificate pair:

Command line window

1. Log in as `root` to the NAC 800 server via SSH.
2. Remove the existing keystore by entering the following at the command line:

   ```
   rm -f /usr/local/nac/keystore/compliance.keystore
   ```

3. Enter the following at the command line:

   ```
   keytool -genkey -keyalg RSA -alias <key_alias> -keystore
   /usr/local/nac/keystore/compliance.keystore
   ```

   Where:

   <*key_alias*> is the name for the key within the keystore file

4. The `keytool` utility prompts you for the following information:
   - Keystore password – Enter a password. You may want to use `changeit` to be consistent with the default password of the J2SE SDK keystore.
   - First and Last Name – Enter the fully-qualified name of your server. This fully-qualified name includes the host name and the domain name. For testing purposes on a single machine, this will be `localhost`.
   - Organizational unit – Enter the appropriate value.
   - Organization – Enter the name of your organization.
   - City or locality – Enter the city or location.
   - State or province – Enter the unabbreviated state or province.
   - Two-letter country code – Enter a two-letter country code. The two-letter country code for the United States is US.
5. Review the information you've entered so far, enter `Yes` if it is correct.

6. The `keytool` utility prompts you for the following information:

   Key password for key_alias – Do not enter a password; press `[Return]` to use the same password that was given for the keystore password.

Using an SSL Certificate from a known Certificate Authority (CA)

To generate a Certificate Signing Request (CSR) to be submitted to a Certificate Authority (CA):

1. Log in as `root` to the NAC 800 server via SSH.
2. Enter the following at the command line:

   keytool -certreq -alias <*key_alias*> -keyalg RSA -file <*csr_filename*> -keystore `/usr/local/nac/keystore/compliance.keystore`

   Where:

   <*key_alias*> is the name for the key within the keystore file

   <*csr_filename*> is the name of the file to store the certificate request

3. `keytool` prompted for the password for the <*keystore_filename*> file, which is the password used when the keystore was created.
4. Submit the CSR (see "Copying Files" on page 1-20) to your chosen CA (such as Thawte or Verisign) along with anything else they might require:

   http://www.verisign.com/
   http://www.thawte.com/

5. If you are using a non-traditional CA (such as your own private Certificate Authority/Public Key Infrastructure (CA/PKI), or if you are using a less well-known CA, you will need to import the CA's root certificate(s) into the java cacerts file by entering the following command on the command line of the NAC 800 server:

   `keytool -import -alias <CA_alias> -file <ca_root_cert_file> -keystore /usr/local/java/jre/lib/security/cacerts`

   Where:

   <*CA_alias*> is an alias unique to your cacerts file and preferably identifies

the CA to which it pertains

<*ca_root_cert_file*> is the file containing the CA's root certificate

6. `keytool` prompts for the password for the cacerts file, which should be the default: `changeit`.
7. If you are prompted, enter `yes` to trust the certificate.
8. Once you get your signed certificate back from the CA, import it into your keystore (see "Copying Files" on page 1-20), replacing the previously self-signed public certificate for your key by entering the following command on the command line of the NAC 800 server:

   ```
   keytool -import -alias <key_alias> -trustcacerts -file
   <signed_cert_file> -keystore /usr/local/nac/keystore/
   compliance.keystore
   ```

   Where:

   <*key_alias*> is the name for the key within the keystore file

   <*signed_cert_file*> is the name of the file containing your CA-signed certificate

9. `keytool` prompts for the password for the keystore_filename file, which is the password used when the keystore was created.
10. Save and exit the file.

Moving an ES from One MS to Another

If you have an existing ES, you can move it to a different MS by performing the steps in this section.

To move an ES to a different MS:

Command line window

1. Log in to the ES as `root` using SSH or directly with a keyboard.
2. Enter the following command at the command line:

   ```
   service nac-es stop
   ```

3. Log in the MS console that currently manages the ES you want to move.
4. Select **System Configuration>>Enforcement clusters & servers**.
5. Click **delete** next to the ES you want to move.
6. In the command line window of the ES, enter the following command:

   ```
   resetSystem.py
   ```

7. Log in to the MS console of the server that you want to manage the ES.
8. Add the ES by following the directions in "Adding an Enforcement Server" on page 3-13.

Recovering Quickly from a Network Failure

If you have a network with a very large number of endpoints (around 3000 endpoints per ES), and your network goes down, perform the following steps to make sure that your endpoints can reconnect as quickly as possible:

1. Place all of the clusters that have a large number of endpoints in allow all mode:
   a. Select **System configuration**.
   b. Click a cluster name.
   c. Select the **allow all** radio button.
   d. Click **ok**.
2. Leave the cluster in allow all mode for a full test cycle. If your test cycle is to retest endpoints every two hours, leave the cluster in allow all mode for two hours. To check the length of your test cycle:
   a. Select **NAC policies**.
   b. Click a policy name.
   c. Select the **Basic settings** menu option.
   d. In the **Retest frequency** area, check the **Retest endpoints every X hours** text field.

NOTE: The retest frequency can be different for each policy.

3. Move the clusters back to normal mode:
   a. Select **System configuration**.
   b. Click a cluster name.
   c. Select the **normal** radio button.
   d. Click **ok**.

Tests Help

Chapter Contents

Overview A-3
Security Settings – Windows A-24
- Allowed Networks A-24
- MS Excel Macros A-24
- MS Outlook Macros A-25
- MS Word Macros A-26
- Mac AirPort Preference A-19
- Mac AirPort User Prompt A-19
- Mac AirPort WEP Enabled A-20
- Mac Bluetooth A-20
- Mac Firewall A-21
- Mac Internet Sharing A-22
- Mac Services A-22
- Services Not Allowed A-27
- Services Required A-28
- Windows Bridge Network Connection A-29
- Windows Security Policy A-30
- Windows Startup Registry Entries Allowed A-32

Software – Windows A-34
- Anti-spyware A-34
- Anti-virus A-35
- High-risk Software A-36
- MS Office Version Check A-36
- P2P A-37
- Personal Firewalls A-37
- Software Not Allowed A-38
- Software Required A-39
- Worms, Viruses, and Trojans A-39

Operating System – Windows A-11
- IIS Hotfixes A-11
- Internet Explorer Hotfixes A-11
- Service Packs A-13

Windows 2000 Hotfixes A-13
Windows Media Player Hotfixes A-14
Windows Server 2003 SP1 Hotfixes A-14
Windows Server 2003 Hotfixes A-15
Windows XP SP2 Hotfixes A-16
Windows XP Hotfixes A-17
Windows Automatic Updates A-17
Browser Security Policy – Windows A-4
Browser Version A-5
Internet Explorer (IE) Internet Security Zone A-6
Internet Explorer (IE) Local Intranet Security Zone A-7
Internet Explorer (IE) Restricted Site Security Zone A-8
Internet Explorer (IE) Trusted Sites Security Zone A-10

Overview

The tests performed on endpoints attempting to connect to the network are listed on the **NAC 800 Home window>>NAC policies>>Select a NAC policy>>Tests**. These tests are updated when you download the latest versions by selecting **NAC 800 Home window>>System Configuration>>Test Updates>>Check for Test Updates.**

This appendix describes tests available to NAC policies. Each section covers one test and describes the following sections:

- Description – An overview of the check performed in this test.
- Test Properties – Information on configuring the criteria which an endpoint must meet to pass the test.
- How Does this Affect Me? – An explanation of the risks that the test attempts to mitigate.
- What Do I Need to Do? – Steps an administrator or user can take to help the endpoint pass the test.

Browser Security Policy – Windows

The Browser security policy tests verify that any endpoint attempting to connect to your system meets your specified security requirements. Browser vulnerabilities are related to cookies, caches, and scripts (JavaScript, Java, and Active scripting / ActiveX). You can specify generally what level of security to enforce (*High*, *Medium*, *Medium-low*, or *Low*) or you can specify exactly what feature to allow or disallow. Installing the most recent version of your browser also helps protect your system against exploits targeting the latest vulnerabilities. table A-1 provides more information about types of browser vulnerabilities:

Item	Description
Cookies	Cookies are text files created by Web sites and stored on your computer. They contain user-specific information—information about what Web pages you visited, information you filled out in online forms, and your preferences for a particular Web site. Cookies are good when they enhance your Web experience (online shopping carts work because of cookies) and can be bad if unencrypted information is stored in them, which could be misused if an attacker gains access to them. The following links provide detailed information about cookies: • http://www.pcworldmalta.com/archive/iss57/cookies.htm • http://www.cookiecentral.com/content.phtml?area=2&id=1
Cache	Cache is a user-specifiable amount of disk space where temporary files are stored. These files contain graphics and Web pages you visit. The primary purposes for storing Web page information is to save time reloading pages and graphics, and to reduce network traffic by not having to repeatedly send the information over the network. Risk occurs if there is sensitive information from encrypted pages stored in the cache, which could be misused if an attacker gains access to the cache files.
Scripts	Scripts and scripting languages are executable code that provides a more interactive Web experience. Some scripts are downloaded to your computer (ActiveX, Java), others are run via the browser (JavaScript).

Table A-1.Browser Vulnerabilities

Item	Description
JavaScript	JavaScript is a scripting language used to enhance Web pages. JavaScript programs are embedded in Web pages and enable active functionality; for example, JavaScript allows you to create images that change when you move the mouse over them and clocks with moving parts. The following links provide more detailed information about JavaScript: • http://www.javascript.com/ • http://javascript.internet.com/ • http://www.javascriptkit.com/
Active scripting / ActiveX	Active scripting / ActiveX extends other programming languages (such as Java) by providing re-usable "controls" that enable developers to make Web pages "active". ActiveX is Microsoft's brand for active scripting. The following links provide more detailed information about ActiveX: • http://www.active-x.com/articles/whatis.htm • http://www.active-x.com/ • http://www.newportinc.com/software/activex/whatisAX.htm
Java	Java is a programming language and a collection of platforms that are targeted toward a specific hardware platform. Java programs are not limited by the operating system (OS) as they are interpreted (run) by another program called the Java Virtual Machine (JVM). This enables Java programs to be portable—that is, they can be run on a server, desktop, personal digital assistant (PDA), or in the browser. The following links provide more information about Java: • http://java.sun.com/learning/new2java/index.html • http://www.javaworld.com/channel_content/jw-topical-index.shtml • http://java.sun.com/

Table A-1.Browser Vulnerabilities

Browser Version

Description

This test verifies that the endpoint attempting to connect to your system has the latest browser version installed.

Test Properties

Select the check box for the required browser software. Enter a version in the text box. If no version is specified in the text box, the default version shown in the square brackets is required.

How Does this Affect Me?

Older browsers may not have adequate security or fixes against vulnerabilities.

What Do I Need to Do?

Install a required browser or update your browser to the required version. See the following links for browser information:

http://www.mozilla.com/en-US/firefox/

http://www.microsoft.com/windows/ie/ie6/default.mspx

Internet Explorer (IE) Internet Security Zone

Description

This test verifies that the endpoint attempting to connect to your system is configured according to your specified Internet security zone standards.

Test Properties

Select the Internet Explorer Internet security zone settings required on your network.

- **High**. Disables all ActiveX Controls and plug-ins, disables file downloads, prompts for font downloads, disables or prompts for Miscellaneous options, disables Scripting, requires login
- **Medium**. A mix of enabled, disabled and prompt for ActiveX controls, enables downloads, a mix of enabled, disabled and prompt for Miscellaneous options, enables Scripting, enables automatic login for intranet
- **Medium-low**. A mix of enabled, disabled and prompt for ActiveX controls, enables downloads, a mix of enabled, disabled and prompt for Miscellaneous options, enables Scripting, enables automatic login for intranet
- **Low**. A mix of enabled and prompt for ActiveX controls, enables downloads, a mix of enabled and prompt for Miscellaneous options, enables Scripting, enables automatic login

How Does this Affect Me?

The Internet security zone defines a security level for all external Web sites that you visit (unless you have specified exceptions in the trusted and restricted site configurations). The default setting is **Medium**.

The following link provides details about the specific security options in the Custom Level window: http://www.microsoft.com/windows/ie/using/howto/security/setup.asp

The following link provides details on how to find and change the settings in IE:

http://www.microsoft.com/windows/ie/using/howto/security/settings.asp

What Do I Need to Do?

1. Select **Tools>>Internet Options>>Security>>Internet**
2. Select **Default Level** to return to the default settings.
3. Select **Custom Level** to specify **High, Medium, Medium-low**, or **Low** or to create custom settings.

Internet Explorer (IE) Local Intranet Security Zone

Description

This test verifies that the endpoint attempting to connect to your system is configured according to your specified local intranet security zone standards.

Test Properties

Select the Internet Explorer local intranet security zone settings required on your network.

- **High**. Disables all ActiveX Controls and plug-ins, disables file downloads, prompts for font downloads, disables or prompts for Miscellaneous options, disables Scripting, requires login
- **Medium**. A mix of enabled, disabled and prompt for ActiveX controls, enables downloads, a mix of enabled, disabled and prompt for Miscellaneous options, enables Scripting, enables automatic login for intranet

- **Medium-low**. A mix of enabled, disabled and prompt for ActiveX controls, enables downloads, a mix of enabled, disabled and prompt for Miscellaneous options, enables Scripting, enables automatic login for intranet
- **Low**. A mix of enabled and prompt for ActiveX controls, enables downloads, a mix of enabled and prompt for Miscellaneous options, enables Scripting, enables automatic login

How Does this Affect me?

The intranet security zone defines a security level for all internal Web sites that you visit (unless you have specified exceptions in the trusted and restricted site configurations). The default setting is **Medium-low**.

The following link provides details about the specific security options in the Custom Level window:

http://www.microsoft.com/windows/ie/using/howto/security/setup.asp

The following link provides details on how to find and change the settings in IE:

http://www.microsoft.com/windows/ie/using/howto/security/settings.asp

What Do I Need to Do?

1. Select **Tools>>Internet Options>>Security>>Intranet**
2. Select one of the following:
   - **Default Level** to return to the default settings.
   - Select **Custom Level** to specify **High, Medium, Medium-low,** or **Low** or to create custom settings.

Internet Explorer (IE) Restricted Site Security Zone

Description

This test verifies that the endpoint attempting to connect to your system is configured according to your specified restricted site security zone standards.

Test Properties

Select the Internet Explorer restricted sites security zone settings required on your network.

- **High**. Disables all ActiveX Controls and plug-ins, disables file downloads, prompts for font downloads, disables or prompts for Miscellaneous options, disables Scripting, requires login
- **Medium**. A mix of enabled, disabled and prompt for ActiveX controls, enables downloads, a mix of enabled, disabled and prompt for Miscellaneous options, enables Scripting, enables automatic login for intranet
- **Medium-low**. A mix of enabled, disabled and prompt for ActiveX controls, enables downloads, a mix of enabled, disabled and prompt for Miscellaneous options, enables Scripting, enables automatic login for intranet
- **Low**. A mix of enabled and prompt for ActiveX controls, enables downloads, a mix of enabled and prompt for Miscellaneous options, enables Scripting, enables automatic login

How Does this Affect Me?

The restricted sites security zone defines a security level for all restricted Web sites that you visit. The default setting is **High.** You also define the specific sites by name and IP address that are restricted. For example, you could specify www.unsafesite.com as a restricted site.

The following link provides details about the specific security options in the Custom Level window:

http://www.microsoft.com/windows/ie/using/howto/security/setup.asp

The following link provides details on how to find and change the settings in IE:

http://www.microsoft.com/windows/ie/using/howto/security/settings.asp

What Do I Need to Do?

1. Select **Tools>>Internet Options>>Security>>Restricted sites**
2. Select one of the following:
   -**Default Level** to return to the default settings.
   - Select **Custom Level** to specify **High, Medium, Medium-low,** or **Low** or to create custom settings.
3. Select **Sites**.
4. Enter a domain name or IP address in the **Add this web site to the zone** text box.

5. Click **Add**.
6. Click **OK**.

Internet Explorer (IE) Trusted Sites Security Zone

Description

This test verifies that the endpoint attempting to connect to your system is configured according to your specified trusted sites security zone standards.

Test properties

Select the Internet Explorer trusted sites security zone settings required on your network.

- **High**. Disables all ActiveX Controls and plug-ins, disables file downloads, prompts for font downloads, disables or prompts for Miscellaneous options, disables Scripting, requires login.
- **Medium**. A mix of enabled, disabled and prompt for ActiveX controls, enables downloads, a mix of enabled, disabled and prompt for Miscellaneous options, enables Scripting, enables automatic login for intranet
- **Medium-low**. A mix of enabled, disabled and prompt for ActiveX controls, enables downloads, a mix of enabled, disabled and prompt for Miscellaneous options, enables Scripting, enables automatic login for intranet
- **Low**. A mix of enabled and prompt ActiveX controls, enables downloads, a mix of enabled and prompt for Miscellaneous options, enables Scripting, enables automatic login

Operating System – Windows

The Operating System (OS) tests verify that any endpoint attempting to connect to your system meets your specified OS requirements. Installing the most recent version of your OS helps protect your system against exploits targeting the latest vulnerabilities.

IIS Hotfixes

Description

Checks for updates to Microsoft Internet Information Services (IIS).

Test Properties

Select the check box for each IIS update to verify. Select the **All critical updates** check box for the most secure option.

How Does this Affect Me?

Hotfixes are programs that update the software and may include performance enhancements, bug fixes, security enhancements, and so on. There is usually only one fix in a hotfix, whereas a patch includes multiple hotfixes.

What Do I Need to Do?

Use the Windows 2000 IIS Hotfix Checking Tool to verify that you have the latest hotfixes:

http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=6C8AFC1C-5008-4AC8-84E1-1632937DBD74

Internet Explorer Hotfixes

Description

Checks for hotfixes to Microsoft Internet Explorer (IE).

Test Properties

Select the hotfixes required on your network. Selecting the **All critical updates option** requires all the critical patches that have been released or will be released by Microsoft.

How Does this Affect Me?

Hotfixes are programs that update the software and may include performance enhancements, bug fixes, security enhancements, and so on. There is usually only one fix in a hotfix, whereas a patch includes multiple hotfixes.

What Do I Need to Do?

Manually initiate an update check (http://v4.windowsupdate.microsoft.com/en/default.asp) if automatic update is not enabled, or is not working.

MVM Hotfixes

Description

Checks for hotfixes to Microsoft Virtual Machine (VM).

Test Properties

Select the hotfixes required on your network. Selecting the **All critical updates option** requires all the critical patches that have been released or will be released by Microsoft.

How Does this Affect Me?

Hotfixes are programs that update the software and may include performance enhancements, bug fixes, security enhancements, and so on. There is usually only one fix in a hotfix, whereas a patch includes multiple hotfixes.

What Do I Need to Do?

Manually initiate an update check (http://v4.windowsupdate.microsoft.com/en/default.asp) if automatic update is not enabled, or is not working.

Service Packs

Description

This test verifies that the endpoint attempting to connect to your system has the latest operating system (OS) service packs installed.

Test Properties

The service packs are listed here by operating system.

How Does this Affect Me?

Service packs are programs that update the software and may include performance enhancements, bug fixes, security enhancements, and so on. There is usually more than one fix in a service pack, whereas a hotfix is usually one fix.

What Do I Need to Do?

Manually initiate an update check (http://v4.windowsupdate.microsoft.com/en/default.asp) if automatic update is not enabled, or is not working.

Windows 2000 Hotfixes

Description

This test verifies that the endpoint attempting to connect to your system has the latest Windows 2000 hotfixes installed.

Test Properties

Select the hotfixes from the list presented that are required on your network. This list will occasionally change as tests are updated. The most secure option is to select the **All critical updates** option, as this requires all the critical patches that have been released or that will be released by Microsoft. You don't have to keep checking by patch number.

How Does this Affect Me?

Hotfixes are programs that update the software and may include performance enhancements, bug fixes, security enhancements, and so on. There is usually only one fix in a hotfix, whereas a patch includes multiple hotfixes.

What Do I Need to Do?

Manually initiate an update check (http://v4.windowsupdate.microsoft.com/en/default.asp) if automatic update is not enabled, or is not working.

Windows Media Player Hotfixes

Description

Checks for Windows Media Player hotfixes.

Test Properties

Select the hotfixes required on your network. Selecting **All critical updates** requires all the critical patches that have been released or will be released by Microsoft.

How Does this Affect Me?

Hotfixes are programs that update the software and may include performance enhancements, bug fixes, security enhancements, and so on. There is usually only one fix in a hotfix, whereas a patch includes multiple hotfixes.

What Do I Need to Do?

Manually initiate an update check (http://v4.windowsupdate.microsoft.com/en/default.asp) if automatic update is not enabled, or is not working.

Windows Server 2003 SP1 Hotfixes

Description

This test verifies that the endpoint attempting to connect to your system has the latest Windows Server 2003 SP1 hotfixes installed.

Test Properties

Select the hotfixes from the list presented that are required on your network. This list will occasionally change as tests are updated. The most secure option is to select the **All critical updates** option, as this requires all the critical patches that have been released or that will be released by Microsoft. You don't have to keep checking by patch number.

How Does this Affect Me?

Hotfixes are programs that update the software and may include performance enhancements, bug fixes, security enhancements, and so on. There is usually only one fix in a hotfix, whereas a patch includes multiple hotfixes.

What Do I Need to Do?

Manually initiate an update check (http://v4.windowsupdate.microsoft.com/en/default.asp) if automatic update is not enabled, or is not working.

Windows Server 2003 SP2 Hotfixes

Description

This test verifies that the endpoint attempting to connect to your system has the latest Windows Server 2003 SP2 hotfixes installed.

Test Properties

Select the hotfixes from the list presented that are required on your network. This list will occasionally change as tests are updated. The most secure option is to select the **All critical updates** option, as this requires all the critical patches that have been released or that will be released by Microsoft. You don't have to keep checking by patch number.

How Does this Affect Me?

Hotfixes are programs that update the software and may include performance enhancements, bug fixes, security enhancements, and so on. There is usually only one fix in a hotfix, whereas a patch includes multiple hotfixes.

What Do I Need to Do?

Manually initiate an update check (http://v4.windowsupdate.microsoft.com/en/default.asp) if automatic update is not enabled, or is not working.

Windows Server 2003 Hotfixes

Description

This test verifies that the endpoint attempting to connect to your system has the latest Windows Server 2003 hotfixes installed.

Test Properties

Select the hotfixes from the list presented that are required on your network. This list will occasionally change as tests are updated. The most secure option is to select the **All critical updates** option, as this requires all the critical patches that have been released or that will be released by Microsoft. You don't have to keep checking by patch number.

How Does this Affect Me?

Hotfixes are programs that update the software and may include performance enhancements, bug fixes, security enhancements, and so on. There is usually only one fix in a hotfix, whereas a patch includes multiple hotfixes.

What Do I Need to Do?

Manually initiate an update check (http://v4.windowsupdate.microsoft.com/en/default.asp) if automatic update is not enabled, or is not working.

Windows XP SP2 Hotfixes

Description

This test verifies that the endpoint attempting to connect to your system has the latest Windows XP SP2 hotfixes installed.

Test Properties

Select the hotfixes from the list presented that are required on your network. This list will occasionally change as tests are updated. The most secure option is to select the **All critical updates** option, as this requires all the critical patches that have been released or that will be released by Microsoft. You don't have to keep checking by patch number.

How Does this Affect Me?

Hotfixes are programs that update the software and may include performance enhancements, bug fixes, security enhancements, and so on. There is usually only one fix in a hotfix, whereas a service pack includes multiple hotfixes.

What Do I Need to Do?

Manually initiate an update check (http://v4.windowsupdate.microsoft.com/en/default.asp) if automatic update is not enabled, or is not working.

Windows XP Hotfixes

Description

This test verifies that the endpoint attempting to connect to your system has the latest Windows XP hotfixes installed.

Test Properties

Select the hotfixes from the list presented that are required on your network. This list will occasionally change as tests are updated. The most secure option is to select the **All critical updates** option, as this requires all the critical patches that have been released or that will be released by Microsoft. You don't have to keep checking by patch number.

How Does this Affect Me?

Hotfixes are programs that update the software and may include performance enhancements, bug fixes, security enhancements, and so on. There is usually only one fix in a hotfix, whereas a service pack includes multiple hotfixes.

What Do I Need to Do?

Manually initiate an update check (http://v4.windowsupdate.microsoft.com/en/default.asp) if automatic update is not enabled, or is not working.

Windows Automatic Updates

Description

This test verifies that the endpoint attempting to connect to your system has Windows Automatic Updates enabled.

Test Properties

Select the minimum setting for Windows automatic updates that is required of endpoints attempting to connect to your network.

- On – Download and install automatically
- On – Download automatically but notify before installing (*Recommended*)
- On – Notify before downloading and installing
- Off – No action taken (*Not recommended*)

How Does this Affect Me?

Microsoft periodically releases software updates to "patch holes" (vulnerabilities) and incorporate other fixes and updates. Although you can manually initiate an update check (http://v4.windowsupdate.microsoft.com/en/default.asp), automatically checking for updates ensures a higher level of security. Updates can be service packs or hotfixes.

Read more about Windows Update here: http://www.microsoft.com/security/protect/update.asp.

What Do I Need to Do?

Enable automatic updates for Windows XP:

http://www.microsoft.com/security/protect/windowsxp/updates.asp

Enable automatic updates for Windows 2000:

1. Select **Start>>Settings>>Control Panel>>Automatic Updates**
2. Select **Keep my computer up to date**.
3. Select **Download the updates automatically and notify me when they are ready to be installed**.
4. Click **OK**.

Security Settings – OS X

Mac AirPort Preference

Description

This test verifies that the Mac AirPort® joins only preferred networks.

Test Properties

There are no properties to set for this test.

How Does this Affect Me?

If you move between different locations, and you use an AirPort network in each one, you can choose your preferred AirPort network for each network location you create. When you move to a different location, your Mac will connect to your preferred AirPort network.

What Do I Need to Do?

Configure the Mac endpoint to join only preferred networks. Select Mac Help, or refer to the following link for assistance on configuring AirPort:

http://www.apple.com/support/airport/

Mac AirPort User Prompt

Description

This test verifies that the user is prompted before joining an open network.

Test Properties

There are no properties to set for this test.

How Does this Affect Me?

If you move between different locations, this option prompts you before automatically joining any network.

What Do I Need to Do?

Configure the Mac endpoint to prompt before joining open networks. Select Mac Help, or refer to the following link for assistance on configuring AirPort:

http://www.apple.com/support/airport/

Mac AirPort WEP Enabled

Description

This test verifies that WEP encryption is enabled for Airport.

Test Properties

There are no properties to set for this test.

How Does this Affect Me?

Wired Equivalent Privacy (WEP) is a wireless network security standard that provides the same level of security as the security in a wired network. WEP encrypts data as it is sent from one endpoint to another. Whenever you use a wireless technology, you should make sure that it is secure so that others cannot access your network.

What Do I Need to Do?

Configure the Mac endpoint to use WEP encryption. Select Mac Help, or refer to the following link for assistance on configuring AirPort:

http://www.apple.com/support/airport/

Mac Bluetooth

Description

This test verifies that Bluetooth is either completely disabled or if enabled is not discoverable.

Test Properties

There are no properties to set for this test.

How Does this Affect Me?

Bluetooth is a wireless technology that allows computers and other devices (such as mobile phones and personal digital assistants (PDAs)) to communicate. Whenever you use a wireless technology, you should make sure that it is secure so that others cannot access your network.

What Do I Need to Do?

Disable Bluetooth, or configure Bluetooth so that it is not discoverable on the endpoint.

Select Mac Help, or refer to the following for assistance on configuring Bluetooth:

http://www.apple.com/bluetooth/

http://www.bluetooth.com/bluetooth/

Mac Firewall

Description

This test verifies that the firewall is enabled.

Test Properties

There are no properties to set for this test.

How Does this Affect Me?

See the description of firewalls under “How Does this Affect Me?” on page A-38.

What Do I Need to Do?

Enable the firewall on the endpoint.

Apple Menu>>System Preferences>>Sharing>>Firewall

1. Select the services and ports you want to allow in the **Allow** area.
2. Click **Start**.

Mac Internet Sharing

Description

This test verifies that the internet sharing is disabled.

Test Properties

There are no properties to set for this test.

How Does this Affect Me?

Mac internet sharing allows one computer to share its internet connection with other computers. This can present security risks by allowing other users to access the network.

What Do I Need to Do?

Disable internet sharing on the endpoint.

Apple Menu>>System Preferences>>Sharing

1. Select the **Internet** tab.
2. Click **Stop**.

Mac Services

Description

This test verifies that the services checked here are allowed on the endpoint.

Test Properties

Select one or more check boxes for services that are allowed on the endpoint.

How Does this Affect Me?

Services are operating system applications that run automatically, without manual intervention.

What Do I Need to Do?

Enable or disable services on the endpoint.

Apple Menu>>System Preferences>>Sharing

1. Select the **Services** tab.
2. Select a service, such as Personal File Sharing.
3. Click **Stop** to turn off sharing for that service, or **Start** to turn on sharing for that service.

Security Settings – Windows

The Security settings tests verify that any endpoint attempting to connect to your system meets your specified security settings requirements.

Allowed Networks

Description

Checks for the presence of an unauthorized connection on a endpoint. These might include connections to a rogue wireless access point, VPN, or other remote network.

Test Properties

Enter a list of IP ranges that are legitimate for your network. Add the ranges separating the start and end IP with a "-". For example, 10.10.1.20-10.10.1.254.

How Does this Affect Me?

Unauthorized connections to your network can allow attackers access to sensitive information on your network or allow them to disrupt network services.

What Do I Need to Do?

Enter the IP address ranges that are allowed for your network.

MS Excel Macros

Description

This test verifies that the endpoint attempting to connect to your system has the Microsoft Excel macro security level specified by your security standards.

Test Properties

Select the minimum Microsoft Excel macro setting for that is required in order for a endpoint to connect to your network.

- **High**. Only signed macros from trusted sources will be allowed to run. Unsigned macros are automatically disabled.

- **Medium**. You can choose whether or not to run potentially unsafe macros.
- **Low**. You are not protected from potentially unsafe macros. (*Not recommended*)

How Does this Affect Me?

Macros are simple programs that are used to repeat commands and keystrokes within another program. A macro can be invoked (run) with a simple command that you assign, such as [ctrl]+[shift]+[r]. Some viruses are macro viruses and are hidden within a document. When you open an infected document, the macro virus runs. A macro virus can save itself to other files (such as the Normal template) and can potentially infect all of your files. If a user on another computer opens the infected file, the virus can spread to their computer as well.

What Do I Need to Do?

Set the Microsoft Excel macro security level as follows:

1. Open Excel.
2. Select **Tools>>Macro>>Security>>Security Level** tab**.**
3. Select **High**, **Medium**, or **Low.**
4. Click **ok**.

MS Outlook Macros

Description

This test verifies that the endpoint attempting to connect to your system has the Microsoft Outlook macro security level specified by your security standards.

Test Properties

Select the minimum Microsoft Outlook macro setting for that is required in order for an endpoint to connect to your network.

- **High**. Only signed macros from trusted sources will be allowed to run. Unsigned macros are automatically disabled.
- **Medium**. You can choose whether or not to run potentially unsafe macros.

- **Low**. You are not protected from potentially unsafe macros. (*Not recommended*).

How Does this Affect Me?

Macros are simple programs that are used to repeat commands and keystrokes within another program. A macro can be invoked (run) with a simple command that you assign, such as [ctrl]+[shift]+[r]. Some viruses are macro viruses and are hidden within a document. When you open an infected document, the macro virus runs. A macro virus can save itself to other files (such as the Normal template) and can potentially infect all of your files. If a user on another computer opens the infected file, the virus can spread to their computer as well.

What Do I Need to Do?

Set the Microsoft Outlook macro security level as follows:

1. Open Outlook.
2. Select **Tools>>Macro>>Security>>Security Level tab.**
3. Select **High, Medium**, or **Low.**
4. Click **ok**.

MS Word Macros

Description

This test verifies that the endpoint attempting to connect to your system has the Microsoft Word macro security level specified by your security standards.

Test Properties

Select the minimum Microsoft Word macro setting for that is required in order for an endpoint to connect to your network.

- **High**. Only signed macros from trusted sources will be allowed to run. Unsigned macros are automatically disabled.
- **Medium**. You can choose whether or not to run potentially unsafe macros.
- **Low**. You are not protected from potentially unsafe macros. (*Not recommended*)

How Does this Affect Me?

Macros are simple programs that are used to repeat commands and keystrokes within another program. A macro can be invoked (run) with a simple command that you assign, such as [ctrl]+[shift]+[r]. Some viruses are macro viruses and are hidden within a document. When you open an infected document, the macro virus runs. A macro virus can save itself to other files (such as the Normal template) and can potentially infect all of your files. If a user on another computer opens the infected file, the virus can spread to their computer as well.

What Do I Need to Do?

Set the Microsoft Word macro security level as follows:

1. Open Word.
2. Select **Tools>>Macro>>Security>>Security Level tab.**
3. Select **High, Medium,** or **Low.**
4. Click **ok**.

Services Not Allowed

Description

This test verifies that the endpoint attempting to connect to your system is running only compliant services.

Test Properties

Enter a list of services that are not allowed on connecting endpoints. Separate additional services with a carriage return. Use the service names found in the **Start>>Settings>>Control Panel>>Administrative Tools>>services** application. For example:

Telnet
Messenger
Remote Desktop Help Session Manager

How Does this Affect Me?

Services are Windows operating system applications that run automatically, without manual intervention.

Services explained:
http://www.microsoft.com/technet/security/guidance/serversecurity/tcg/tcgch07n.mspx

How to identify the services running in a process:
http://www.microsoft.com/resources/documentation/windows/2000/server/scriptguide/en-us/sas_ser_arwi.mspx

Tips on Windows XP services:
http://www.theeldergeek.com/services_guide.htm

What do I need to do?

For services you never use, disable the service. For services you may use occasionally, change the startup type from automatic to manual.

How to change the service startup type:

1. Select **Start>>Settings>>Control Panel>>Administrative Tools>>Services**.
2. Right-click on a service and select **Properties**.
3. Select **Manual** or **Disabled** from the **Startup type** drop-down list.
4. Click **OK**.
5. Close the **Services** window.
6. Close the **Administrative Tools** window.

Services Required

Description

This test verifies that the endpoint attempting to connect to your system is running the services specified by your security standards.

Test Properties

Enter a list of services that are required for connecting endpoints. Separate additional services with a carriage return. Use the service names found in the **Start>>Settings>>Control Panel>>Administrative Tools>>services** application. For example:

Telnet
Messenger
Remote Desktop Help Session Manager

How Does this Affect Me?

Services are Windows operating system applications that run automatically, without manual intervention.

Services explained:
http://www.microsoft.com/technet/security/guidance/serversecurity/tcg/tcgch07n.mspx

How to identify the services running in a process:
http://www.microsoft.com/resources/documentation/windows/2000/server/scriptguide/en-us/sas_ser_arwi.mspx

Tips on Windows XP services:
http://www.theeldergeek.com/services_guide.htm

What Do I Need to Do?

For services you always use, change the startup type to automatic.

How to change the service startup type:

1. Select **Start>>Settings>>Control Panel>>Administrative Tools>>Services**.
2. Right-click on a service and select **Properties**.
3. Select **Automatic** from the **Startup type** drop-down list.
4. Click **OK**.
5. Close the **Services** window.
6. Close the **Administrative Tools** window.

Windows Bridge Network Connection

Description

This test verifies that the endpoint attempting to connect to the network does not have a bridged network connection present. A bridged network connection allows the connecting endpoint to transparently send traffic to and from another network. An example use of this type of connection would be to bridge a high-speed cellular network connection in and out of the local network. A bridged network connection poses a significant security risk.

Test Properties

Any endpoint which has a Windows bridge Network Connection will fail this test.

How Does this Affect Me?

Using network bridges can be useful in some environments; however, they also create a security risk.

What Do I Need to Do?

Do not use network bridges.

The following articles describe bridge networking:

http://technet2.microsoft.com/windowsserver/en/library/df594316-cd92-4c38-9773-4c6d74e02a431033.mspx?mfr=true

http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/hnw_understanding_bridge.mspx?mfr=true

http://www.microsoft.com/windowsxp/using/networking/expert/crawford_02april22.mspx

Windows Security Policy

Description

This test verifies that the endpoint attempting to connect to your system follows the Windows local security policy best practices.

Test Properties

Select the Windows local security policy options you want to require on your network.

- Enable "Network access: Do not allow storage of credentials or .NET Passports for network authentication"
- Disable "Network access: Let Everyone permissions apply to anonymous users"
- Enable "Accounts: Limit local account use of blank passwords to console logon only"

How Does this Affect Me?

Certain configurations, such as the ones listed above, create potential holes that can leak sensitive information if your system is compromised. Selecting the above policy options creates a more secure network environment. The following links provide detailed information on these security settings:

- Enable "Network access: Do not allow storage of credentials or .NET Passports for network authentication"
  http://technet2.microsoft.com/windowsserver/en/library/66a6776a-b1ef-43dd-8f18-d694fd07494b1033.mspx?mfr=true
- Disable "Network access: Let Everyone permissions apply to anonymous users"
  http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/loc_sec_set.mspx?mfr=true
- Enable "Accounts: Limit local account use of blank passwords to console logon only"
  http://www.microsoft.com/resources/documentation/IIS/6/all/proddocs/en-us/Default.asp?url=/resources/documentation/IIS/6/all/proddocs/en-us/636.asp

What Do I Need to Do?

To select the security policies:

1. Select **Start>>Settings>>Control Panel>>Administrative Tools**.
2. Double-click **Local Security Policy**.
3. Double-click **Local Policies**.
4. Double-click **Security Options**.
5. Double-click a security policy.
6. Select **Enabled** or **Disabled**.
7. Click **OK**.
8. Close the **Local Security Settings** window.
9. Close the **Administrative Tools** window.

Windows Startup Registry Entries Allowed

Description

This test verifies that the endpoint attempting to connect to your system does not contain non-compliant registry entries in the run and runOnce Windows registry keys.

Test Properties

Enter a list of registry key and values that are allowed in the run and runOnce Windows registry keys. If the endpoint has any other values in those keys, the test will fail. Separate entries by semicolons in the format <key> or <key>::<value>.

For example:

updater::C:\Program Files\Common files\Updater\wupdater.exe

will allow Windows update to run on startup.

How Does this Affect Me?

The Microsoft Windows Registry contains information that Windows uses during normal operations, including system options, property settings, applications installed, types of documents each application can create, ports used, and so on. Information is stored in keys, such as run and runOnce. The run and runOnce keys cause programs to run automatically. Many worms and viruses are started by a call from the Windows Registry. If you limit what can start up when you log in, you can reduce the potential for worms and viruses to run on your system.

The following links provide a description of the Microsoft Windows Registry and the Run keys:

- http://support.microsoft.com/default.aspx?scid=kb;EN-US;256986
- http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/q137/3/67.asp&NoWebContent=1
- http://support.microsoft.com/default.aspx?scid=kb;EN-US;314866
- http://www.winguides.com/registry/

What Do I Need to Do?

Verify that the run and runOnce registry keys run only compliant programs.

CAUTION: Modifying registry entries incorrectly can cause serious problems that may require you to reinstall your operating system.

1. Back up the registry as described at the following links:
   XP and Windows Server 2003 – http://support.microsoft.com/default.aspx?scid=kb;EN-US;322756
   2000 – http://support.microsoft.com/default.aspx?scid=kb;EN-US;322755
   NT 4.0 – http://support.microsoft.com/default.aspx?scid=kb;EN-US;323170
2. Open the Registry editor by selecting **Start>>Run**.
3. Type `regedit` and click **OK**.
4. Select **Edit>>Find**. Search for the run and runOnce keys:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
   HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ RunServices
   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ RunServicesOnce
   HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ RunOnce\Setup
5. If the keys have any other value than the one specified, delete the unauthorized value by double-clicking the item, deleting the data, and clicking **OK**.

TIP: If you're looking for a registry key, you enter a trailing slash. If you're looking for a registry value, you do not enter a trailing slash.

Software – Windows

The Software tests verify that any endpoint attempting to connect to your system meets your specified software requirements. Installing the most recent version of your software helps protect your system against exploits targeting the latest vulnerabilities.

Anti-spyware

Description

This test verifies that the endpoint attempting to connect to your system has anti-spyware tools installed and that the anti-spyware definitions are up-to-date.

Test Properties

Select the anti-spyware software allowed on your network. Any endpoint that does not have at least one of the anti-spyware software packages selected will fail this test. You can also enter a value in the **Last scan performed within** text field, which requires the anti-spyware software to have executed a scan on the endpoint within the set number of days.

How Does this Affect Me?

Spyware is software that gathers and transmits information (about the user, computer, and/or network) without the user's knowledge. It is usually installed without the user's knowledge through seemingly harmless downloads such as freeware, shareware, instant messages, and email attachments. Spyware is intentionally difficult to detect and remove. Those who create and release spyware don't want you to know it's there or be able to easily uninstall it. The information gathered can be exploited for mischief, for financial gain, and for gaining unauthorized access to your network. Spyware also consumes system resources and can cause system instability and crashes.

What Do I Need to Do?

Make sure you have an anti-spyware program installed, that the spyware definitions are kept up-to-date, and that your system is scanned often.

Anti-virus

Description

This test verifies that the endpoint attempting to connect to your system has the latest anti-virus software installed, that it is running, and that the virus definitions are up-to-date.

Test Properties

Select the anti-virus software allowed on your network. Any endpoint that does not have at least one of the anti-virus software packages selected will fail this test. You can also enter a value in the **Last scan performed within** text field, which requires the anti-virus software to have executed a scan on the endpoint within the set number of days.

How Does this Affect Me?

Anti-virus software scans your computer, email, and other files for known viruses, worms, and trojan horses. It searches for known files and automatically removes them. A virus is a program that infects other programs and files and can spread when a user opens a program or file containing the virus. A virus needs a host (the program or file) to spread.

A worm is a program that can also perform malicious acts (such as delete files and send email); however, it replicates itself and does not need a host (program or file) to spread. Frequently, worms are used to install a backdoor (a way for an attacker to gain access without having to login).

A trojan horse is a stand-alone program that is not what it seems. For example, it may seem to be calendar program, but when you open it, it erases all your files and displays a message, such as "Ha ha, I deleted your files!" Trojan horse programs do not spread or replicate themselves.

What Do I Need to Do?

Make sure you have an anti-virus program installed, and that the virus definitions are kept up-to-date.

The following link provides more information on anti-virus software and protecting your computer: http://www.us-cert.gov/cas/tips/ST04-005.html

High-risk Software

Description

This test verifies that the endpoint attempting to connect to your system does not have High-risk software installed.

Test Properties

Select the high-risk software not allowed on your network. Any endpoint that has at least one of the high-risk software packages selected fails this test.

How Does this Affect Me?

Some software provides security risks, such as allowing data to be stored on external servers, or not encrypting sensitive data.

What Do I Need to Do?

Remove or disable any disallowed high-risk software.

MS Office Version Check

Description

This check fetches the version and service pack information of the Microsoft Office software installed.

Test Properties

Select the check box for one or more Microsoft Office packages. Any software package selected that does not have the latest version installed fails the test.

How Does this Affect Me?

Some companies may support only the software listed. Using the most recently updated version of software can help protect your system from known vulnerabilities.

What Do I Need to Do?

Verify that you have updated software by visiting the following link:

http://office.microsoft.com/en-us/downloads/default.aspx

P2P

Description

This test verifies that the endpoint attempting to connect to your system has only approved person-to-person (P2P) software installed.

Test Properties

Select the P2P software allowed on your network. If none of the P2P packages are selected, this means that you do not allow P2P software and any endpoint with P2P software enabled will fail this test.

How Does this Affect Me?

A Peer-to-peer (P2P) network is one that is comprised of peer nodes (computers) rather than clients and servers. These peer nodes function both as clients and servers to other nodes and can perform any client or server function. P2P software allows users to connect directly to other users and is used for file sharing. Many P2P software packages are considered spyware and their use is generally discouraged.

What Do I Need to Do?

Remove or disable any disallowed P2P software.

Personal Firewalls

Description

This test verifies that the endpoint attempting to connect to your system has the latest personal firewall software installed and running.

Test Properties

Select the personal firewall(s) that meet your requirements. Any endpoint that does not have at least one of the personal firewalls selected will fail this test.

How Does this Affect Me?

A firewall is hardware or software that views information as it flows to and from your computer. You configure the firewall to allow or block data based on criteria such as port number, content, source IP address, and so on.

The following links provide more detailed information about firewalls:

- http://computer.howstuffworks.com/firewall.htm
- http://www.pcstats.com/articleview.cfm?articleid=1450&page=4
- http://www.microsoft.com/technet/network/wf/default.mspx
- http://www.firewallguide.com/

What Do I Need to Do?

Make sure you have a personal firewall installed.

Software Not Allowed

Description:

This test verifies that the endpoint attempting to connect to your system does not have the software packages listed installed.

Test Properties

Enter a list of applications that are not allowed on connecting endpoints, separated with a carriage return. The format for an application is vendor\software package[\version]. Using this format stores the value in the HKEY_LOCAL_MACHINE\Software key.

For example:

Adobe\Acrobat Reader, Adobe\Acrobat Reader\6.0

You can also specify which key to use for the specific value by entering the key at the beginning of the value. For example:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Messenger

How Does this Affect Me?

Some software is generally not appropriate for corporate use, and can create vulnerabilities in your system, for example, peer-to-peer (P2P) software and instant messenging (IM) software.

What Do I Need to Do?

Remove the software that is not allowed.

Software Required

Description

This test verifies that the endpoint attempting to connect to your system has the required software packages installed.

Test Properties

Enter a list of applications that are required on all connecting endpoints, separated with a carriage return. The format for an application is vendor\software package[\version]. Using this format stores the value in the HKEY_LOCAL_MACHINE\Software key.

For example:

Adobe\Acrobat Reader, Adobe\Acrobat Reader\6.0

You can also specify which key to use for the specific value by entering the key at the beginning of the value. For example:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Messenger

How Does this Affect Me?

Connecting to a network may be impossible if the correct software is not installed and operational.

What Do I Need to Do?

Contact the vendor and install the missing software.

Worms, Viruses, and Trojans

Description:

This test verifies that the endpoint attempting to connect to your system does not have any of the worms, viruses, or trojans listed.

Test Properties

This area of the window displays the current list of worms, viruses, and trojans. No selection actions are required.

How Does this Affect Me?

A virus is a program that infects other programs and files and can spread when a user opens a program or file containing the virus. A virus needs a host (the program or file) to spread. A worm is a program that can also perform malicious acts (such as delete files and send email); however, it replicates itself—it does not need a host (program or file) to spread. Frequently, worms are used to install a backdoor (a way for an attacker to gain access without having to login). A trojan horse is a stand-alone program that is not what it seems. For example, it may seem to be calendar program, but when you open it, it erases all your files and displays a message, such as "Ha ha, I deleted your files!" Trojan horse programs do not spread or replicate themselves.

What Do I Need to Do?

Make sure you are running an anti-virus software program, and that it is kept up-to-date.

Important Browser Settings

Chapter Contents

Pop-up Windows B-2
Active Content B-3
Minimum Font Size B-5
Page Caching B-6
Temporary Files B-7

Pop-up Windows

The NAC 800 reports capability uses a pop-up window. In order for you to run reports on NAC 800, you *must* allow pop-up windows from the NAC 800 server.

To allow pop-up windows in IE 6.0 with SP2:

IE browser>>Tools>>Pop-up blocker>>Pop-up blocker settings

1. Enter the IP address or partial IP address of NAC 800.
2. Click **Add**.
3. Click **Close**.

To allow pop-up windows in Mozilla:

Mozilla browser>>Edit>>Preferences>>Privacy & Security>>Allowed sites

1. Enter the IP address or partial IP address of NAC 800.
2. Click **Add**.
3. Click **OK**.
4. Click **OK**.

To allow pop-up windows in Firefox:

Firefox browser>>Tools>>Options>>Content

1. Deselect the **Block Popup Windows** checkbox.
2. Click **OK**.

Active Content

The Windows® XP Service Pack 2 (SP2) installation changes some of the Internet Explorer (IE) browser's security settings. This change in settings causes the message (figure B-1), to display at the top of the browser window when you access the NAC 800 help feature.

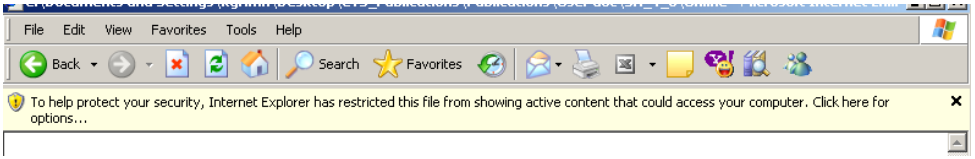

File Edit View Favorites Tools Help
Back
Search
Favorites
To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for options...

Figure B-1. Internet Explorer Security Warning Message

To view the NAC 800 online help in IE:

1. Click on the message box to display the options:

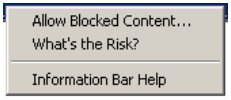


Figure B-2. IE Security Message Options

2. Select the **Allow Blocked Content** option. The **Security Warning** window appears:

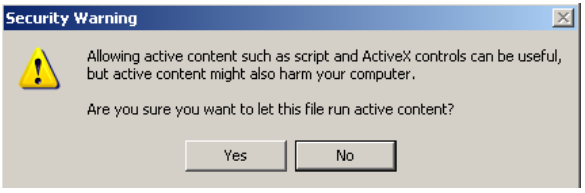

Security Warning
Allowing active content such as script and ActiveX controls can be useful, but active content might also harm your computer.
Are you sure you want to let this file run active content?
Yes
No

Figure B-3. IE Security Warning Pop-up Window

3. Click **Yes**.

To change the IE security settings to always allow active content:

IE browser>>Tools>>Options>>Advanced tab

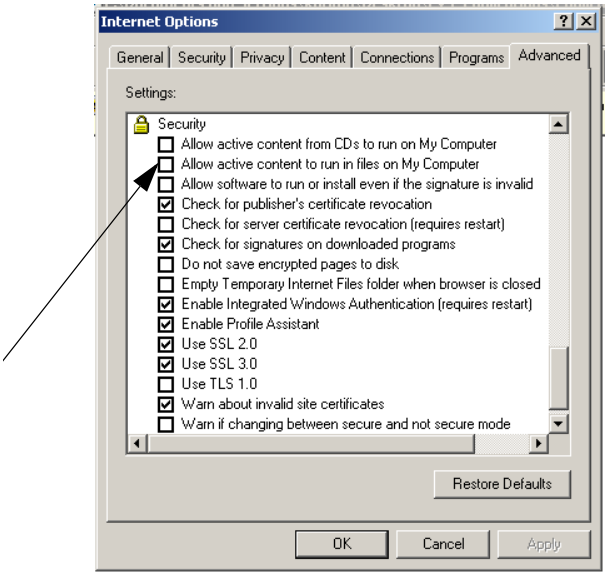


Figure B-4. IE Internet Options, Advanced Tab

1. Scroll down to the security section.
2. Select the **Allow active content to run in files on my computer** check box.
3. Click **OK**.

Minimum Font Size

In order to properly display the NAC 800 console, do not specify the minimum font size.

To clear the IE minimum font size:

IE browser>>Tools>>Internet options>>General tab>>Accessibility button

1. Make sure all of the check boxes are cleared on this window.
2. Click **OK**.
3. Click **OK**.

To clear the Mozilla minimum font size:

Mozilla browser>>Edit>>Preferences>>Appearance>>Fonts

1. Select **None** from the **Minimum font size** drop-down list.
2. Click **OK**.

To clear the Firefox minimum font size:

Firefox browser>>Tools>>Options>>Content>>Advanced

1. Ensure that **Allow pages to choose their own fonts, instead of my selections above** from the **Fonts** pop-up window is selected.
2. Click **OK**.
3. Click **OK**.

Page Caching

To set the IE page caching options:

Internet Explorer browser>>Tools>>Internet Options

1. On the **General** tab, click **Settings**.
2. Under **Check for new versions of stored pages**, select the **Automatically** radio button.
3. Click **OK**.
4. In the **Internet Options** dialog box, click the **Advanced** tab.
5. In the **Security** options, make sure that **Do not save encrypted pages to disk** is *not* checked.
6. Click **OK**.

Temporary Files

Periodically delete temporary files from your system to improve browser performance.

To delete temporary files in IE:

Internet Explorer>>Tools>>Internet Options>>General tab

1. Click **Delete Files**.
2. Select the **Delete all offline content** check box.
3. Click **OK**.
4. Click **OK**.

To delete temporary files in Mozilla:

Mozilla browser>>Edit>>Preferences

1. Select the plus (+) symbol next to **Advanced** to expand the topic.
2. Select **Cache**.
3. Click **Clear Cache**.

To delete temporary files in Firefox:

Firefox browser>>Tools>>Options

1. Select the **Privacy** icon at the left of the window.
2. Select **Cache**.
3. Click **Clear Cache Now**.
4. Click **OK**.

(This page intentionally left blank.)

Installation and Configuration Check List

Chapter Contents

Minimum System Requirements C-2
IP Addresses, Hostname, Logins, and Passwords C-3
Single-server Installation C-3
Multiple-server Installations C-3
Proxy Server C-6
Agentless Credentials C-78
Quarantine C-8
802.1X C-8
802.1X Devices C-9
DHCP C-10
Accessible services C-10
Notifications C-12
Test Exemptions C-13

Minimum System Requirements

Required fields are indicated by a red asterisk (*).

- ❒ Internet connection with outbound SSL communications *
  NOTE: You must have access to the following:
  - ❒ For license validation and test updates:
    update.hp.com port 443 *
  - ❒ For software and operating system updates:
    download.hp.com port 80 *
- ❒ Workstation running one of the following browsers with 128-bit encryption: *
  - ❒ Windows:
    Mozilla Firefox 1.5 or later
    Mozilla 1.7
    Internet Explorer 6.0
  - ❒ Linux:
    Mozilla Firefox 1.5 or later
    Mozilla 1.7
- ❒ ProCurve NAC Endpoint Integrity Agent License *
- ❒ ProCurve NAC Implementation Start-up Service, from an authorized ProCurve partner or ProCurve

IP Addresses, Hostname, Logins, and Passwords

Required fields are indicated by a red asterisk (*).

Single-server Installation

The MS and ES are installed on the same physical server (appliance).

- ❒ MS/ES IP address: * _____
- ❒ MS/ES Netmask IP address (Network mask): * _____
- ❒ Cluster name: * _____
- ❒ Default gateway IP address: * _____
- ❒ Primary nameserver IP address (DNS server): * _____
- ❒ Secondary nameserver IP address (DNS server): _____
- ❒ Tertiary nameserver IP address (DNS server): _____
- ❒ MS/ES hostname (FQDN): * _____

TIP: Select simple names that are short, easy to remember, have no spaces or underscores, and the first and last character cannot be a dash (-).

- ❒ Time zone: * _____
- ❒ MS/ES server root password: * _____
- ❒ MS/ES Database password:* _____
- ❒ NAC 800 console administrator account name: * _____
- ❒ NAC 800 console administrator account password: * _____
- ❒ SMTP server IP address: _____

Multiple-server Installations

The MS is installed on one physical server (appliance); each ES is installed on a unique physical server (appliance).

Management Server

Create at least one MS.

- ❒ MS IP address: * _____

- ❒ MS Netmask IP address (Network mask): * _____
- ❒ Default gateway IP address: * _____
- ❒ Primary nameserver IP address (DNS server): * _____
- ❒ Secondary nameserver IP address (DNS server): _____
- ❒ Tertiary nameserver IP address (DNS server): _____
- ❒ MS hostname (FQDN): * _____

TIP: Select simple names that are short, easy to remember, have no spaces or underscores, and the first and last character cannot be a dash (-).

- ❒ Time zone: * _____
- ❒ MS server root password: * _____
- ❒ MS Database password:* _____
- ❒ NAC 800 console administrator account name: * _____
- ❒ NAC 800 console administrator account password: * _____
- ❒ SMTP server IP address: _____

Enforcement Server 1

Create at least one ES.

- ❒ Cluster name 1: * _____
- ❒ ES IP address: * _____
- ❒ ES Netmask IP address (Network mask): * _____
- ❒ Default gateway IP address: * _____
- ❒ Primary nameserver IP address (DNS server): * _____
- ❒ Secondary nameserver IP address (DNS server): _____
- ❒ Tertiary nameserver IP address (DNS server): _____
- ❒ ES hostname (FQDN): * _____

TIP: Select simple names that are short, easy to remember, have no spaces or underscores, and the first and last character cannot be a dash (-).

- ❒ Time zone: * _____
- ❒ ES server root password: * _____
- ❒ ES Database password:* _____

- ❒ NAC 800 console administrator account name: * _____
- ❒ NAC 800 console administrator account password: * _____

Enforcement Server 2

Create at least one ES.

- ❒ Cluster name 2: * _____
- ❒ ES IP address: * _____
- ❒ ES Netmask IP address (Network mask): * _____
- ❒ Default gateway IP address: * _____
- ❒ Primary nameserver IP address (DNS server): * _____
- ❒ Secondary nameserver IP address (DNS server): _____
- ❒ Tertiary nameserver IP address (DNS server): _____
- ❒ ES hostname (FQDN): * _____
- ❒ Time zone: * _____
- ❒ ES server root password: * _____
- ❒ ES Database password:* _____
- ❒ NAC 800 console administrator account name: * _____
- ❒ NAC 800 console administrator account password: * _____

Enforcement Server 3

Create at least one ES.

- ❒ Cluster name 3: * _____
- ❒ ES IP address: * _____
- ❒ ES Netmask IP address (Network mask): * _____
- ❒ Default gateway IP address: * _____
- ❒ Primary nameserver IP address (DNS server): * _____
- ❒ Secondary nameserver IP address (DNS server): _____
- ❒ Tertiary nameserver IP address (DNS server): _____
- ❒ ES hostname (FQDN): * _____
- ❒ Time zone: * _____
- ❒ ES server root password: * _____

- ❒ ES Database password: * _____
- ❒ NAC 800 console administrator account name: * _____
- ❒ NAC 800 console administrator account password: * _____

Proxy Server

If you use a proxy server for Internet connections, these fields are required:

- ❒ Proxy server IP address: *_____
- ❒ Proxy server port: * _____
- ❒ Proxy server authentication method (basic or digest): *_____
- ❒ Proxy server user ID: * _____
- ❒ Proxy server password: * _____

Agentless Credentials

Required fields are indicated by a red asterisk (*).

The administrator credentials for endpoints on a domain. Set them globally for all clusters, or override them on a per-cluster basis.

- ❒ All clusters:
  - ❒ Windows domain name: * _____
  - ❒ Administrator user ID: * _____
  - ❒ Administrator password: * _____
- ❒ Cluster 1:
  - ❒ Windows domain name: * _____
  - ❒ Administrator user ID: * _____
  - ❒ Administrator password: * _____
- ❒ Cluster 2:
  - ❒ Windows domain name: * _____
  - ❒ Administrator user ID: * _____
  - ❒ Administrator password: * _____
- ❒ Cluster 3:
  - ❒ Windows domain name: * _____
  - ❒ Administrator user ID: * _____
  - ❒ Administrator password: * _____
- ❒ Cluster 4:
  - ❒ Windows domain name: * _____
  - ❒ Administrator user ID: * _____
  - ❒ Administrator password: * _____

Quarantine

Required fields are indicated by a red asterisk (*).

Define quarantine methods and settings for all clusters, or on a per-cluster basis.

802.1X

- ❒ IDM Server IP address _____
- ❒ Quarantine subnets: * _____
- ❒ RADIUS server type (local or remote IAS): * _____
- ❒ Local RADIUS server type end-user authentication method:
  - ❒ Manual: _____
  - ❒ Windows domain:
    - ❒ Domain name: * _____
    - ❒ Administrator user name: * _____
    - ❒ Administrator password: * _____
    - ❒ Domain controllers: * _____
    - ❒ Additional credentials user name: * _____
    - ❒ Additional credentials password: * _____
  - ❒ Open LDAP:
    - ❒ Server: * _____
    - ❒ Identity: * _____
    - ❒ Password: * _____
    - ❒ Base DN: * _____
    - ❒ Filter: * _____
    - ❒ Password attribute: * _____
    - ❒ End-user credentials user name: * _____
    - ❒ End-user credentials Password: * _____
  - ❒ Novell eDirectory:
    - ❒ Server: * _____

- ❒ Identity: * _____
- ❒ Password: * _____
- ❒ Base DN: * _____
- ❒ Filter: * _____
- ❒ Password attribute: * _____
- ❒ End-user credentials user name: * _____
- ❒ End-user credentials Password: * _____

802.1X Devices

Define 802.1X devices globally for all clusters, or on a per-cluster basis.

- ❒ 802.1X device 1
  - ❒ IP address: * _____
  - ❒ Shared secret: * _____
  - ❒ Device type: * _____
- ❒ 802.1X device 2
  - ❒ IP address: * _____
  - ❒ Shared secret: * _____
  - ❒ Device type: * _____
- ❒ 802.1X device 3
  - ❒ IP address: * _____
  - ❒ Shared secret: * _____
  - ❒ Device type: * _____
- ❒ 802.1X device 4
  - ❒ IP address: * _____
  - ❒ Shared secret: * _____
  - ❒ Device type: * _____
- ❒ 802.1X device 5
  - ❒ IP address: * _____
  - ❒ Shared secret: * _____
  - ❒ Device type: * _____

DHCP

Define quarantine areas for all clusters, or on a per-cluster basis. Create as many quarantine areas as you need.

NOTE: If you select DHCP quarantine, you must create at least one area or you will get a process error.

- ❒ DHCP quarantine area 1:*
  - ❒ Quarantine area 1 quarantined subnet: *_____
  - ❒ Quarantine area 1 DHCP IP range: * _____
  - ❒ Quarantine area 1 quarantined area gateway: *_____
  - ❒ Quarantine area 1 domain suffix: *_____
  - ❒ Quarantine area 1 corresponding non-quarantined subnets: * _____
- ❒ DHCP quarantine area 2:
  - ❒ Quarantine area 2 quarantined subnet: _____
  - ❒ Quarantine area 2 DHCP IP range: * _____
  - ❒ Quarantine area 2 quarantined area gateway: _____
  - ❒ Quarantine area 2 domain suffix: *_____
  - ❒ Quarantine area 2 corresponding non-quarantined subnets: _____
- ❒ DHCP quarantine area 3:
  - ❒ Quarantine area 3 quarantined subnet: _____
  - ❒ Quarantine area 3 DHCP IP range: * _____
  - ❒ Quarantine area 3 quarantined area gateway: _____
  - ❒ Quarantine area 3 domain suffix: *_____
  - ❒ Quarantine area 3 corresponding non-quarantined subnets: _____

Accessible services

Accessible services are defined for all clusters, or on a per-cluster basis.

- ❒ Accessible services and endpoints for all clusters:
  - ❒ Web sites:_____

- ❒ Hostnames: _____
- ❒ IP addresses / ports: _____
- ❒ Networks: _____
- ❒ Windows domain controller: _____

❒ Accessible services and endpoints for cluster 1:

- ❒ Web sites: _____
- ❒ Hostnames: _____
- ❒ IP addresses / ports: _____
- ❒ Networks: _____
- ❒ Windows domain controller: _____

❒ Accessible services and endpoints for cluster 2:

- ❒ Web sites: _____
- ❒ Hostnames: _____
- ❒ IP addresses / ports: _____
- ❒ Networks: _____
- ❒ Windows domain controller: _____

❒ Accessible services and endpoints for cluster 3:

- ❒ Web sites: _____
- ❒ Hostnames: _____
- ❒ IP addresses / ports: _____
- ❒ Networks: _____
- ❒ Windows domain controller: _____

Notifications

Required fields are indicated by a red asterisk (*).

Notifications are defined for all clusters, or on a per-cluster basis.

- ❒ All clusters
  - ❒ Send information to: _____
  - ❒ SNMP server IP address: _____
  - ❒ Email information sent from:_____
- ❒ Cluster 1
  - ❒ Send information to: _____
  - ❒ SNMP server IP address: _____
  - ❒ Email information sent from:_____
- ❒ Cluster 2
  - ❒ Send information to: _____
  - ❒ SNMP server IP address: _____
  - ❒ Email information sent from:_____
- ❒ Cluster 3
  - ❒ Send information to: _____
  - ❒ SNMP server IP address: _____
  - ❒ Email information sent from:_____

Test Exemptions

Required fields are indicated by a red asterisk (*).

Exemptions are defined for all clusters, or on a per-cluster basis.

- ❒ All cluster endpoint testing exemptions (endpoints that are always allowed access or always quarantined):
  - ❒ MAC addresses: _____
  - ❒ IP addresses: _____
  - ❒ NetBIOS names: _____
- ❒ Cluster 1 endpoint testing exemptions (endpoints that are always allowed access or always quarantined):
  - ❒ MAC addresses: _____
  - ❒ IP addresses: _____
  - ❒ NetBIOS names: _____
- ❒ Cluster 2 endpoint testing exemptions (endpoints that are always allowed access or always quarantined):
  - ❒ MAC addresses: _____
  - ❒ IP addresses: _____
  - ❒ NetBIOS names: _____
- ❒ Cluster 3 endpoint testing exemptions (endpoints that are always allowed access or always quarantined):
  - ❒ MAC addresses: _____
  - ❒ IP addresses: _____
  - ❒ NetBIOS names: _____

(This page intentionally left blank.)

Glossary

The following terms and definitions are used in this book, and in other ProCurve Management Software documentation.

802.1X: A port-based authentication protocol that can dynamically vary encryption keys, and has three components: a supplicant, an authenticator, and an authentication server.

NAC policies: In NAC 800, NAC policies consist of individual tests that evaluate endpoints attempting to access the network. These tests assess operating systems, verify that key hotfixes and patches have been installed, ensure anti-virus and other security applications are present and up-to-date, detect the presence of worms, trojans, and viruses, and check for potentially dangerous applications such as file sharing, peer-to-peer (P2P), or spyware.

NAC policy group: A logical grouping of NAC policies.

ACL: Access control list – A list or set of rules that routers (and other networking endpoints) use to control and regulate access through the endpoint and subsequently onto the network.

ACS: Access Control Server

ActiveX: A Microsoft technology that enables interactive Web content.

agent: An information exchange process that works in conjunction with clients and servers to perform tasks.

API: Application Programming Interface

backdoor: A disguised or hidden entry point in a software program or system. An open backdoor can be intentional (for maintenance use), or unintentional. If a backdoor is discovered, malicious users or software can gain entry and cause damage.

cache: A location where information is stored that can be accessed quickly. This location can be in memory or in a file.

CD: Compact disc

CIDR: Classless InterDomain Routing – a method of specifying networks and sub networks (subnets) that allows grouping and results in less router overhead.

client: A computer that requests services from another (server).

cluster: A logical grouping of Enforcement servers.

compliance: Meets defined standards or conditions.

CTA: Cisco Trust Agent

Enforcement: cluster: A logical grouping of Enforcement servers.

Enforcement: server: When using NAC 800 in a multiple-server installation, the server that is used for enforcement.

ES: Enforcement server

DC: Domain controller – A server that manages and controls the activities (such as user access) in the domain.

DHCP: Dynamic Host Configuration Protocol – A method of assigning IP addresses to endpoints as they connect to the network, and releasing them as the endpoints disconnect from the network. DHCP allows administrators to manage IP addresses from one location rather than at each endpoint.

DN: Distinguished Name – In the Lightweight Directory Access Protocol (LDAP), objects are referenced by their DN.

DNS: Domain name server – A computer that translates domain names (such as mycompany.com) into IP addresses (such as 216.239.41.99).

HA: High Availability – A multiple-server NAC 800 deployment is mutually supporting. Should one server fail, other nodes within a cluster will automatically provide coverage for the affected network segment.

HTML: Hyper text markup language – A language that tells a web browser how to display the web page.

IE: Internet Explorer

IP: Internet protocol – A protocol by which data is sent from one computer to another on the Internet.

IPSec: IP security

ISO image file: An image of a CD saved in ISO 9660 standard format.

IT: Information technology

JMS: Java Message Service – a Java-based message interface.

L2TP: Layer two tunneling protocol – An open standard protocol used to create virtual private networks (VPN).

LAN: Local Area Network

LDAP: Lightweight Directory Access Protocol (LDAP) – A protocol that is used to look up information from a database that usually contains information about authorized users and their privileges.

Load balancing: Load balancing is achieved by an algorithm that spreads the endpoint testing load across all Enforcement servers in a cluster.

MAC: Media Access Control – The unique number that identifies a physical endpoint. Generally referred to as the MAC address.

Management server: When using NAC 800 in a multiple-server installation, the server that is used for managing Enforcement servers.

MS: Management server

multinet A physical network of two or more logical networks.

NAC: Network Admission Control

non-compliance: Does not meet defined standards or conditions.

NTP: Network time protocol – A protocol that ensures local time-keeping.

OS: Operating system

P2P: Person-to-person or Peer-to-peer – A Peer-to-peer (P2P) network is one that is comprised of peer nodes (computers) rather than clients and servers. These peer nodes function both as clients and servers to other nodes and can perform any client or server function. P2P software allows users to connect directly to other users and is used for file sharing. Many P2P software packages are considered spyware and their use is generally discouraged.

PPTP: Point-to-point tunneling protocol – A tunneling protocol used to connect Windows NT clients and servers.

quarantine: In NAC 800, isolating endpoints or systems to prevent potential infection of other endpoints or systems.

RAM: Random access memory

RAS: Remote access server

RDBMS: Relational Database Management System (RDBMS) – used to store information in related tables.

RPC: Remote procedure call – a procedure where arguments or parameters are sent to a program on a remote system. The remote program executes and returns the results.

server: A computer that provides services to another (client).

SMTP: Simple mail transfer protocol – A TCP/IP protocol used in sending and receiving email. Used in conjunction with POP3 or IMAP.

SSH: Secure shell or secure socket shell – A UNIX-based command interface and protocol used to securely gain access to a remote computer.

SSL: Secure socket layer – A commonly-used protocol that manages the security of message transmissions over the Internet.

subnet: A section of a network that shares part of the IP address of that network.

SUS: Software Update Service

temporary access period: In NAC 800, a temporary period of time where an end-user is allowed access.

VPN: Virtual private network – A secure method of using the Internet to gain access to an organization's network.

(This page intentionally left blank.)

Index

Index

Numerics

3rd-party software, installing *15*
802.1X *2, 4*
    communication flow *4*
    configuring the RADIUS server *10*
    connections *2*
    enable *50, 43*
    enable XP endpoint *44, 45, 46*
    installing the RADIUS server *8*
    logging levels, set *112*
    setting up the authenticator *47*
    setting up the RADIUS server *7*
    setting up the supplicant *44*
    test connection *61*

A

access
    always grant *101*
access control status
    granted access *9*
access mode, changing *5*
access period, temporary *38*
access point *2*
access screens, view end-user *106*
access status *9*
    and lease expiration *18*
    disconnected *9*
    has temporary access *9*
    quarantined *9*
    temporary
        quarantine *9*
accessible endpoints, define *98*
accessible services
    define *98*
    determining *6*
ACLs *5*
act on a endpoint *15*
action
    quarantine *16*
    select *15*
    send an email *16*
active content
    allowing *3*
    in the browser *3*
Active Directory *8*
    and IAS *10*
ActiveX *8, 9*
    testing method *96*
add
    custom tests *13*
    Enforcement cluster *7*
    Enforcement server *13*
    NAC policy group *5*
    quarantine area *87*
    user account *29*
    user role *37*
administrator account's user registry settings *109*
agent *8, 9*
    manually install *20*
    remove Mac OS *29*
    removing *20*
    testing *17*
    testing method *96*
    verify Mac OS *25*
    version *21*
Agent read timeout period, set *114*
agent-based testing *17*
agentless *8*
    login credentials *30*
    settings required *6*
    test and Windows Messenger Service *31*
    test method *6*
    testing method *96*
allow
    access without testing *13*
    active content *3*
    pop-up windows *2*
always
    allow access to an endpoint without testing *13*

grant access *101*
quarantine an endpoint without testing *15*
always quarantine
domains *102*
endpoints *102*
AP *2*
assign endpoints and domains to a policy *13*
authentication
information *109*
server *2*
Authenticator *2*
authenticators, define *12*
authorization DLL file *32*

B

backup *91*
system and data *10*
BaseTests API *28*
BasicTests API *28*
browser
allow pop-ups *2*
and active content *3*
end-user *4*
end-user version *106*
important settings *3*
pop-ups required for reports *5*
settings *1*
version *4*
button
check for test updates *4*
configure system *7, 9, 10, 11, 15, 17, 18, 19, 20, 24, 26, 27*
copy policy *12*
generate report *5*
printable report *5*

C

cancel testing *36*
certificate *26*
Certificates *2*
change
MS root password *26*
MS SNMP settings *26*
properties *7*
check for available test updates settings *47*
CIDR *9*
clear a temporary state *17*
client *2*
communication flow, 802.1X *4*
configuration
DHCP *4*
timeout *16*
Windows XP Professional firewall *9, 10*
configure
non-HP switches *40*
proxy RADIUS requests *37, 40*
Windows domain settings *52*
connections, 802.1X *2*
connector, IAS *25*
console timeout, changing *27*
converting reports to MS Word doc *9*
copy
existing NAC policy *12*
user account *33*
create
custom test script *18*
new NAC policy *7*
credentials
delete Windows *110*
edit Windows *109*
for agentless test *30*
login *107*
sort Windows area *110*
test Windows *109*
Windows *107*
custom test
adding *13*
class script from scratch *18*
customize
end-user access screens *105, 106*
the error messages *40*

D

date and time
change ES *17*
DC
name *100*
ports to specify *100*
default
NAC policy *4, 7*
define accessible services and endpoints *98*
delay
login *18*

three minute *18*
delete
cluster *11*
ES *20*
NAC policy *13*
NAC policy group *6*
quarantine area *90*
user account *36*
user role *41*
details, view report *6*
DHCP
configuration *4*
ports to specify *100*
server IP address *100*
DHCP mode and MAC address *102*
directory, end-user template *15*
disable a NAC policy *7*
disconnected *9*
display limited endpoints *6*
documentation *14*
domain
controller *107*
matching policies *5*
Domain Controller
IP address *100*
specifying the name *100*
domains, always quarantine *102*
download the latest tests *4*
downloading support packages *94*

E

EAP *2*
type *19*
EAPOL *2*
edit
end-user access screen *33*
Enforcement cluster *9*
Enforcement server *15*
existing NAC policy *5*
NAC policy *12*
quarantine area *89*
test results messages *33*
user account *34*
user role *40*
email
notification received by *12*
notifications *103*
server *8*
set up notification *103*
specifying server *8*
email notifications
disable *103*
enable *102*
enable
802.1X *50*, *43*
a NAC policy *7*
dll file *32*
file and printer sharing *6*
the Authorization DLL file *32*
Windows XP Professional endpoint for 802.1X *44*, *45*, *46*
endpoint
act on *15*
allow access without testing *13*
always quarantine *102*
assign to policy *13*
end-user supported *3*
immediately grant access *16*
immediately quarantine *17*
managed *9*
quarantine hierarchy *2*
quarantine without testing *15*
retest *16*
unmanaged *9*
view information *18*
endpoints per ES *5*
end-user
access templates *15*
access window *15*
admin password *31*, *35*
endpoints supported *3*
error
screens *38*
file and print sharing *6*
firewall *9*
footer *106*
IE Internet security zone *5*
installing screen *17*
introduction *105*
opening screen *16*
ports *8*
quarantine screen *35*
required firewall settings *12*
specify browser version *19*
test successful message *106*

test successful screen *34*
testing failed screen *37*
view access screens *106*
end-user access screens
customize *105, 106*
editing *33*
viewing *33*
end-user options, selecting *98*
end-user screen
specify logo *104*
specify test failed pop-up *106*
specify text *105*
end-user template directory *15*
Enforcement cluster
add *7*
delete *11*
edit *9*
view statistics *10*
Enforcement server
add *13*
change date and time *17*
change network settings *17*
change password *18*
delete *20*
edit *15*
view status *19*
enforcement, set DHCP *85*
enforcing ranges *39*
Enhanced Security Configuration option, disable *8*
error
ActiveX *30*
message, customize *40*
messages, changing *13*
error screens *38*
ES
logging levels, set *111*
moving *45*
per cluster *5*
per MS *5*
extending existing tests *13*

F

File and Print Sharing *11*
file and printer sharing, enabling *6*
filter
by time *6*
endpoint activity window *5*
find services names *18*
Firefox, supported version *2*
firewall
changing port *14*
letting RPC service through *9*
settings *9*
testing the end-user through *12*
testing through *9*
XP configuration *9, 10*
firewall & end-user *9*
FQDN *3, 4, 5*

G

generate
a CSR *43*
report *4*
granted access *9*

H

has temporary access *9*
help
online *14*
tests *17*
hierarchy
endpoint quarantine *2*
NAC policy *14*
high security *4*
host name in a NAC policy *10*
HTML or text editor *15*

I

IAS
add to Windows Server 2003 Installation *8*
and Active Directory *10*
Connector *25*
IAS posture
Checkup *29*
Healthy *29*
Infected *29*
Quarantined *29*
Unknown *29*
IDM logging levels, set *112*
ignoring ranges *39*
immediately
grant access to an endpoint *16*

quarantine an endpoint *17*
import
certificate *26*
the server's certificate *26*
inactive, set time *14*
INI file, connector *28*
inline *2*
install
agent manually *20*
naming *6*
screen *17*
installing *15*
IP address, static *34*
IPSec *12*

K

Kerberos *2*
key features *10*

L

L2TP *12*
launch and log into *3*
lease expiration *18*
and access status *18*
short times *18*
license
agreement, violation of *15*
updating *43*
validation and test updates *2*
limit endpoints displayed *6*
Linux *3*
log out *3*
login *3*
credentials *107, 30*
delay *18*
domain *107*
save *98*
saving *31*
timeout *14*
Logo *105*
logs, view test update *47*
low security *4*

M

MAC address
in a NAC policy *10*
in DHCP mode *102*
Mac OS *3*
Mac OS agent
remove *29*
verify *25*
managed endpoint *9*
manually test an endpoint *16*
maximum
endpoints per ES *5*
ES per cluster *5*
ES per MS *5*
medium security *4*
minimum
browser version, specify *19*
font size *5*
modify
MS settings *23*
the view *4*
monitoring ranges *39*
move
an ES *45*
NAC policy to new set *13*
Mozilla, supported version *2*
MS, view status *21*

N

NAC policies *2*
window, view *2*
NAC policy
add group *5*
assign domains to *13*
assign endpoint to *13*
assign endpoints to *13*
copy *12*
create *7*
create new *7*
defined *10*
delete *13*
disable *7*
edit *5, 12*
enable *7*
enable/disable *7*
group, delete *6*
hierarchy *14*
high security *4*
host name *10*

low security 4
MAC address 10
medium security 4
move to new set 13
NetBIOS name 10
select default 7
name
Enforcement server 6
MS host 6
NetBIOS in a NAC policy 10
network
naming, CIDR format 9
settings, change ES 17
non-supported operating systems 15
notifications
server 8
specifying email server 8

O

one-time passwords 2
online help 14
viewing 3
opening screen 16
operating systems
non-supported 15
not tested 8
supported 18
ordering test methods 97

P

page caching 6
password
change ES 18
change MS root 26
changing 37
configure for Active Directory 33
end-user admin 31, 35
reset 37
reset console 37
reset root 36
Perl 13
pop-up window 2
allowing 2
port
88 33
88,changing 33
changing firewall 14
enter a range 5
number in quarantined network 4
number, accounting 12
number, authentication 12
ports 8
controlled by AP 3
to specify for DHCP and DC 100
posture
Checkup 29
Healthy 29
Infected 29
Quarantined 29
Unknown 29
PPTP 12
print a report 7
process flow 10
properties
changing 7
set test 15
test 17
protocol supported 12
proxy
RADIUS 40
RADIUS requests 37
server 24
Public key authentication 2
Python 13

Q

quarantine
endpoint without testing 15
method, select 49
network port number 4
screen 35
set up multiple areas 89
quarantine area
add 87
delete 90
edit 89
sort 89
quarantined 9

R

RADIUS 2
authentication method, setting 51

built-in *40*
configure *10*
server and SA plug-in *7*
use existing server *37*
using a proxy *7*
using built-in *7*
range
entering ports *5*
of IP addresses *100*
ranges
to enforce *39*
to ignore *39*
to monitor *39*
refresh *7*
regedit *18*
registry *17*
keys *18*
remote access logging *24*
Remote Access Policy, configure *22*
remove
Mac OS agent *29*
the agent *20*
re-naming installation *6*
report
convert HTML to Word *9*
convert to DOC *9*
generate *4*
NAC policy results *2*
options *4*
print *7*
save *6, 7, 8*
Test details *2*
Test results *2*
Test results by IP address *2*
Test results by netbios name *3*
Test results by user *3*
view details *6*
reports *2*
converting to MS Word doc *9*
enable browser pop-ups *5*
reset
a database *11*
console password *37*
password *37*
system *6*
restore
original database *11*
system and data *10*
retest
an endpoint *16*
set time *14*
time *9*
router *5*
RPC *8*
command timeout period, set *115*
connection timeout period, set *114*
service *9, 10*

S

SAIASConnector.ini *29*
save
a report *8*
login *98*
login information *31*
search *7*
for user account *32*
select
default NAC policy *7*
test method *95*
the action to take *15*
server
certificate *26*
for email notifications *8*
names *100*
services
find names *18*
not allowed *18*
required *18*
services, Agent *20*
set
802.1X logging levels *112*
action to take *15*
Agent read timeout period *114*
connection time *14*
DHCP
setting enforcement *85*
ES logging levels *111*
IDM logging levels *112*
RADIUS authentication method *51*
retest time *14*
RPC command timeout period *115*
RPC connection timeout period *114*
the test properties *15*
time an end-user can be inactive *14*
time to wait before retesting *14*

settings
802.1X, entering 51
change MS SNMP 26
modify MS 23
required for agentless 6
Windows 2003 Server 8
shared services 17
SMTP server IP address 103
software
and operating system updates 2
installing 3rd-party 15
not allowed 17
registry keys 18
required 17
sort
quarantine area 89
user account area 33
user role area 42
specifying an email server for notifications 8
SSH 15
SSL 12
standard tests 2
static IP addresses 34
status access 9
Strings.py 40
Supplicant 2
support package
downloading 94
generate 11
supported
end-user endpoints 3
operating systems 18
protocols 12
VPNs 12
switch
Cisco 2950 47
configure non-HP 40
Enterasys Matrix 1H582-25 49
Extreme Summit 48si 49
Foundry Fast Ironedge 2402 51
restrict access at 5
sample configurations 47
system upgrades 27

T

tcpdump 6
technical support
contacting 13
template location 15
templates 15
changes during upgrade 15
edit and customize 15
renaming 16, 15
temporarily quarantined 9
temporary
access period 38
files 7
state, clearing 17
temporary files 7
test
add custom 13
base functionality 28
connection to 802.1X device 61
creating a custom script 18
properties, selecting 17
set properties 15
status 10
successful screen 34
update times, select 46
updates, checking for 45
test method
ActiveX error 30
agent 17
agent-based 17
select 95
select order 97
test methods
defined 8
options 11
pros & cons 8
to display 98
testing
cancel 36
failed screen 37
ports
used 8
testing method
ActiveX 96
agent 96
agentless 96
tests 2
adding custom 13
entering IE version number 19
entering service names 18
entering software names 17

extending existing *13*
help *17*
standard *2*
updating *4*
viewing help *17*
three-minute delay *18*
time
between tests *9*
set automatically *25*
set connection *14*
set manually *25*
set retest *14*
zone set *26*
timeout *16*
change console *27*
login *14*
Tokens *2*
troubleshooting browser settings *3*

U

unmanaged endpoint *9*
untested endpoint *8, 18*
and lease expiration *18*
update
server names *100*
setting frequency *47*
tests *4*
updates *15*
upgrades *15, 27*
user account
add *29*
copy *33*
delete *36*
edit *34*
search *32*
sort area *33*
user accounts
create Active Directory *34*
Dial-in access & Encryption *35*
user name, changing *37*
user role
add *37*
delete *41*
edit *40*
sort area *42*
user-based tests *109*

V

vi *15*
view
access status *14*
current list of tests *17*
endpoint information *18*
Enforcement cluster statistics *10*
ES status *19*
MS status *21*
NAC policies window *2*
online help *3*
report details *6*
test update logs *47*
tests information *17*
VPNs supported *12*

W

warranty *ii*
window
end-user access *15*
Windows
2000 *3*
2003 Server settings *8*
95 *3, 8*
98 *3*
credentials *107*
domain and end-user settings *5*
domain settings, configure *52*
Group policy *9*
ME *3, 8*
Messenger Service *31*
NT *3*
registry *17*
Server (2000, 2003) *3*
Update server *100*
XP Home *3*
XP Professional *3*
windowsupdate.com *100*

X-Z

XP firewall configuration *9, 10*

(This page intentionally left blank.)

© Copyright 2007 Hewlett-Packard Development Company, L.P.

August 2007

Manual Part Number
5991-8571